TRAITE DE COOPERATION EN MATIERE DE BREVETS

Expéditeur: le BUREAU INTERNATIONAL

PCT

NOTIFICATION D'ELECTION

(règle 61.2 du PCT)

Destinataire:

Assistant Commissioner for Patents
United States Patent and Trademark Office
Box PCT
Washington, D.C.20231
ETATS-UNIS D'AMERIQUE

en sa qualité d'office élu

Date d'expédition (jour/mois/année) 30 août 2000 (30.08.00)	
Demande internationale no PCT/FR00/00188	**Référence du dossier du déposant ou du mandataire** 5343ter.WO
Date du dépôt international (jour/mois/année) 27 janvier 2000 (27.01.00)	**Date de priorité** (jour/mois/année) 27 janvier 1999 (27.01.99)
Déposant GUILLOU, Louis etc	

1. L'office désigné est avisé de son élection qui a été faite:

[X] dans la demande d'examen préliminaire international présentée à l'administration chargée de l'examen préliminaire international le:

19 juillet 2000 (19.07.00)

[ ] dans une déclaration visant une élection ultérieure déposée auprès du Bureau international le:

2. L'élection [X] a été faite

[ ] n'a pas été faite

avant l'expiration d'un délai de 19 mois à compter de la date de priorité ou, lorsque la règle 32 s'applique, dans le délai visé à la règle 32.2b).

Bureau international de l'OMPI **34, chemin des Colombettes** **1211 Genève 20, Suisse**	Fonctionnaire autorisé Antonia Muller
no de télécopieur: (41-22) 740.14.35	no de téléphone: (41-22) 338.83.38

09/889958 Translation

8

PATENT COOPERATION TREATY

PCT

INTERNATIONAL PRELIMINARY EXAMINATION REPORT

(PCT Article 36 and Rule 70)

Applicant's or agent's file reference 5343ter.WO	FOR FURTHER ACTION	See Notification of Transmittal of International Preliminary Examination Report (Form PCT/IPEA/416)
International application No. PCT/FR00/00188	International filing date (*day/month/year*) 27 January 2000 (27.01.00)	Priority date (*day/month/year*) 27 January 1999 (27.01.99)
International Patent Classification (IPC) or national classification and IPC H04L /		
Applicant FRANCE TELECOM		

1. This international preliminary examination report has been prepared by this International Preliminary Examining Authority and is transmitted to the applicant according to Article 36.

2. This REPORT consists of a total of 6 sheets, including this cover sheet.

   ☒ This report is also accompanied by ANNEXES, i.e., sheets of the description, claims and/or drawings which have been amended and are the basis for this report and/or sheets containing rectifications made before this Authority (see Rule 70.16 and Section 607 of the Administrative Instructions under the PCT).

   These annexes consist of a total of 28 sheets.

3. This report contains indications relating to the following items:

   - I ☒ Basis of the report
   - II ☐ Priority
   - III ☐ Non-establishment of opinion with regard to novelty, inventive step and industrial applicability
   - IV ☐ Lack of unity of invention
   - V ☒ Reasoned statement under Article 35(2) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement
   - VI ☐ Certain documents cited
   - VII ☐ Certain defects in the international application
   - VIII ☒ Certain observations on the international application

Date of submission of the demand	Date of completion of this report
19 July 2000 (19.07.00)	15 May 2001 (15.05.2001)
Name and mailing address of the IPEA/EP Facsimile No.	Authorized officer Telephone No.

INTERNATIONAL PRELIMINARY EXAMINATION REPORT

International application No.
PCT/FR00/00188

I. Basis of the report

1. This report has been drawn on the basis of (*Replacement sheets which have been furnished to the receiving Office in response to an invitation under Article 14 are referred to in this report as "originally filed" and are not annexed to the report since they do not contain amendments.*):

☐ the international application as originally filed.

☒ the description, pages 1-52, as originally filed,
pages _____, filed with the demand,
pages _____, filed with the letter of _____,
pages _____, filed with the letter of _____.

☒ the claims, Nos. _____, as originally filed,
Nos. _____, as amended under Article 19,
Nos. _____, filed with the demand,
Nos. 1-24, filed with the letter of 10 January 2001 (10.01.2001),
Nos. _____, filed with the letter of _____.

☐ the drawings, sheets/fig _____, as originally filed,
sheets/fig _____, filed with the demand,
sheets/fig _____, filed with the letter of _____,
sheets/fig _____, filed with the letter of _____.

2. The amendments have resulted in the cancellation of:

☐ the description, pages _____
☐ the claims, Nos. _____
☐ the drawings, sheets/fig _____

3. ☐ This report has been established as if (some of) the amendments had not been made, since they have been considered to go beyond the disclosure as filed, as indicated in the Supplemental Box (Rule 70.2(c)).

4. Additional observations, if necessary:

V. Reasoned statement under Article 35(2) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement

1. Statement

Novelty (N)	Claims	1-24	YES
	Claims		NO
Inventive step (IS)	Claims	1-24	YES
	Claims		NO
Industrial applicability (IA)	Claims	1-24	YES
	Claims		NO

2. Citations and explanations

The invention relates to a method (claim 1) and a system (claims 9 and 17) for proving the authenticity of an entity, and/or the integrity of a message associated therewith, to a verifier entity, using a series of steps involving commitment calculations by a witness device, the reception of challenges by the witness, and the calculation of responses by the witness for verification by the verifier. The invention further relates to a verifier device (claim 21) using the method.

Prior art:

Document EP-A-0 311 470, cited in the application, describes such a method wherein an entity known as a 'trusted authority' assigns an identity to each so-called 'witness' entity and calculates the RSA signature thereof; during a customisation process, the trusted authority provides the witness with an identity and a signature. Thereafter, the witness states: "Here is my identity; I know its RSA signature". The witness proves that it knows the RSA signature of its identity without disclosing it. The public RSA verification key distributed by the trusted authority enables a so-called 'verifier' entity to verify that the RSA signature matches the stated identity without

said signature being disclosed to said entity. The mechanisms that use this method operate "without knowledge transfer", meaning that the witness does not know the private RSA key with which the trusted authority signs a large number of identities. The method uses private values Qi and public values Gi linked by a generic equation $Gi.Gi^{v} = 1. \text{ mod. } N$ (where v is a public exponent).

Problem:

The workload resulting from RSA arithmetic operations leads to excessively long calculation times for smart card applications.

Invention:

The method does not use the RSA signature and calculates the commitments R, challenges d and responses R from the public/private values G_i and Q_i defined according to the features of claim 1.
None of the documents cited in the international search report discloses or suggests the calculation steps defined in claim 1. In particular, EP-A-0 792 044 (X document) also relates to a challenge/response authentication method but it uses RSA technology.
Therefore, the subject matter of claim 1 involves an inventive step (PCT Article 33(3)).

Independent claims 9 and 17 refer to claim 1 in terms of systems comprising the witness device that calculates commitments, receives challenges and calculates responses. Therefore, they too comply with the requirements of PCT Article 33.

Independent claim 21 relates to a verifier device using

calculations G_i and Q_i specific to the method of the invention. Since these calculations are not disclosed or suggested in the cited documents, said claim also complies with the requirements of PCT Article 33.

The other claims are dependent claims and thus also comply, as such, with the requirements of novelty and inventive step of the PCT.

VIII. Certain observations on the international application

The following observations on the clarity of the claims, description, and drawings or on the question whether the claims are fully supported by the description, are made:

The following claims do not fully comply with the requirements of clarity of PCT Article 6, for the following reasons:

1. Independent claim 1:

Since the verification step performed by the 'verifier' entity is not indicated in the claim, the definition of the subject matter of the invention ("method for proving the authenticity of an entity and/or the integrity of a message to a verifier entity") is unclear, given that the features in the claim merely relate to the calculations of the commitment/challenge/response values useful in the authentication method according to the invention.

2. Independent claims 9 and 17 contain the same features as claim 1, but express them in terms of a system and a terminal device, respectively, comprising the witness device that calculates the commitments and the responses to received challenges. Therefore, the objection raised in paragraph 1 above is also applicable to these claims.

3. Independent claim 21 relates to a verifier device for interaction with the witness or terminal device. However, instead of containing device or system features, it contains method or process features, some of which are also external to the system claimed ("unknown to the verifier device").

VIII. Certain observations on the international application

Furthermore, this claim does not comprise the challenge generating means necessary for the authentication process described in the description as a whole. Therefore, independent claim 21 fails to comply with the requirements of PCT Article 6 in combination with PCT Rule 6.3(b), according to which an independent claim must contain all of the technical features essential for the definition of the invention.

TRAITE DE COOPERATION EN MATIERE DE BREVETS 09/889958

PCT

RAPPORT DE RECHERCHE INTERNATIONALE

(article 18 et règles 43 et 44 du PCT)

Référence du dossier du déposant ou du mandataire	POUR SUITE A DONNER voir la notification de transmission du rapport de recherche internationale (formulaire PCT/ISA/220) et, le cas échéant, le point 5 ci-après	
5343ter.WO		
Demande internationale n°	Date du dépôt international *(jour/mois/année)*	(Date de priorité (la plus ancienne) *(jour/mois/année)*
PCT/FR 00/ 00188	27/01/2000	21/01/1999
Déposant		
FRANCE TELECOM et al.		

Le présent rapport de recherche internationale, établi par l'administration chargée de la recherche internationale, est transmis au déposant conformément à l'article 18. Une copie en est transmise au Bureau international.

Ce rapport de recherche internationale comprend 4 feuilles.

[X] Il est aussi accompagné d'une copie de chaque document relatif à l'état de la technique qui y est cité.

1. **Base du rapport**

   a. En ce qui concerne la **langue**, la recherche internationale a été effectuée sur la base de la demande internationale dans la langue dans laquelle elle a été déposée, sauf indication contraire donnée sous le même point.

   [ ] la recherche internationale a été effectuée sur la base d'une traduction de la demande internationale remise à l'administration.

   b. En ce qui concerne **les séquences de nucléotides ou d'acides aminés** divulguées dans la demande internationale (le cas échéant), la recherche internationale a été effectuée sur la base du listage des séquences :

   [ ] contenu dans la demande internationale, sous forme écrite.

   [ ] déposée avec la demande internationale, sous forme déchiffrable par ordinateur.

   [ ] remis ultérieurement à l'administration, sous forme écrite.

   [ ] remis ultérieurement à l'administration, sous forme déchiffrable par ordinateur.

   [ ] La déclaration, selon laquelle le listage des séquences présenté par écrit et fourni ultérieurement ne vas pas au-delà de la divulgation faite dans la demande telle que déposée, a été fournie.

   [ ] La déclaration, selon laquelle les informations enregistrées sous forme déchiffrable par ordinateur sont identiques à celles du listage des séquences présenté par écrit, a été fournie.

2. [ ] **Il a été estimé que certaines revendications ne pouvaient pas faire l'objet d'une recherche** (voir le cadre I).

3. [ ] **Il y a absence d'unité de l'invention** (voir le cadre II).

4. En ce qui concerne le **titre**,

   [X] le texte est approuvé tel qu'il a été remis par le déposant.

   [ ] Le texte a été établi par l'administration et a la teneur suivante:

5. En ce qui concerne l'**abrégé**,

   [ ] le texte est approuvé tel qu'il a été remis par le déposant

   [X] le texte (reproduit dans le cadre III) a été établi par l'administration conformément à la règle 38.2b). Le déposant peut présenter des observations à l'administration dans un délai d'un mois à compter de la date d'expédition du présent rapport de recherche internationale.

6. La figure **des dessins** à publier avec l'abrégé est la Figure n° _____

   [ ] suggérée par le déposant.

   [ ] parce que le déposant n'a pas suggéré de figure.

   [ ] parce que cette figure caractérise mieux l'invention.

   [ ] Aucune des figures n'est à publier.

Cadre III TEXTE DE L'ABREGE (suite du point 5 de la première feuille)

Abrégé

La preuve est établie au moyen des paramètres suivants:

- m couples de valeurs privées Q_i et publiques P_i, m>1
- un module public n constitué par le produit de f facteurs premiers p_i, f>2,
- un exposant public v,

liés par des relations du type:

$$G_i \cdot Q_i^v \equiv 1 \bmod n \quad \text{ou} \quad G_i \equiv Q_i^v \bmod n.$$

RAPPORT DE RECHERCHE INTERNATIONALE

Demande internationale No
P[redacted]R 00/00188

A. CLASSEMENT DE L'OBJET DE LA DEMANDE
CIB 7 H04L9/32

Selon la classification internationale des brevets (CIB) ou à la fois selon la classification nationale et la CIB

B. DOMAINES SUR LESQUELS LA RECHERCHE A PORTE

Documentation minimale consultée (système de classification suivi des symboles de classement)
CIB 7 H04L

Documentation consultée autre que la documentation minimale dans la mesure où ces documents relèvent des domaines sur lesquels a porté la recherche

Base de données électronique consultée au cours de la recherche internationale (nom de la base de données, et si réalisable, termes de recherche utilisés)

C. DOCUMENTS CONSIDERES COMME PERTINENTS

Catégorie °	Identification des documents cités, avec, le cas échéant, l'indication des passages pertinents	no. des revendications visées
X A	EP 0 792 044 A (FUJI XEROX CO LTD) 27 août 1997 (1997-08-27) colonne 9, ligne 39 -colonne 12, ligne 38 figure 3	1,9,17, 22 2,10,18, 23
A	WO 96 33567 A (GEMPLUS CARD INT ;NACCACHE DAVID (FR)) 24 octobre 1996 (1996-10-24) page 2, ligne 27 -page 4, ligne 12 page 15, ligne 31 -page 18, ligne 17	3,4,11, 12,19, 20,24
A	WO 89 11706 A (NCR CO) 30 novembre 1989 (1989-11-30) page 10, ligne 2 -page 11, ligne 6 page 12, ligne 21 -page 14, ligne 6	3,4,11, 12,19, 20,24

-/--

[X] Voir la suite du cadre C pour la fin de la liste des documents

[X] Les documents de familles de brevets sont indiqués en annexe

° Catégories spéciales de documents cités:

"A" document définissant l'état général de la technique, non considéré comme particulièrement pertinent

"E" document antérieur, mais publié à la date de dépôt international ou après cette date

"L" document pouvant jeter un doute sur une revendication de priorité ou cité pour déterminer la date de publication d'une autre citation ou pour une raison spéciale (telle qu'indiquée)

"O" document se référant à une divulgation orale, à un usage, à une exposition ou tous autres moyens

"P" document publié avant la date de dépôt international, mais postérieurement à la date de priorité revendiquée

"T" document ultérieur publié après la date de dépôt international ou la date de priorité et n'appartenenant pas à l'état de la technique pertinent, mais cité pour comprendre le principe ou la théorie constituant la base de l'invention

"X" document particulièrement pertinent; l'inven tion revendiquée ne peut être considérée comme nouvelle ou comme impliquant une activité inventive par rapport au document considéré isolément

"Y" document particulièrement pertinent; l'inven tion revendiquée ne peut être considérée comme impliquant une activité inventive lorsque le document est associé à un ou plusieurs autres documents de même nature, cette combinaison étant évidente pour une personne du métier

"&" document qui fait partie de la même famille de brevets

Date à laquelle la recherche internationale a été effectivement achevée	Date d'expédition du présent rapport de recherche internationale
31 mars 2000	19/04/2000

Nom et adresse postale de l'administration chargée de la recherche internationale	Fonctionnaire autorisé
Office Européen des Brevets, P.B. 5818 Patentlaan 2 NL – 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Masche, C

Formulaire PCT/ISA/210 (deuxième feuille) (juillet 1992)

C.(suite) DOCUMENTS CONSIDERES COMME PERTINENTS

Catégorie *	Identification des documents cités, avec, le cas échéant, l'indicationdes passages pertinents	no. des revendications visées
A	EP 0 311 470 A (TELEDIFFUSION FSE ;FRANCE ETAT (FR); PHILIPS NV (NL)) 12 avril 1989 (1989-04-12) cité dans la demande abrégé colonne 12, ligne 30 -colonne 13, ligne 55	1,9,17, 22
A	QUISQUATER J -J ET AL: "FAST DECIPHERMENT ALGORITHM FOR RSA PUBLIC-KEY CRYPTOSYSTEM" ELECTRONICS LETTERS, vol. 18, no. 21, 14 octobre 1982 (1982-10-14), pages 905-907, XP000577331 ISSN: 0013-5194 page 906, colonne de gauche, ligne 32 - ligne 61	1,6,9, 14,17

RAPPORT DE RECHERCHE INTERNATIONALE

Renseignements relatifs aux mem[redacted]de familles de brevets

Demande internationale No
P[redacted]R 00/00188

Document brevet cité au rapport de recherche	Date de publication	Membre(s) de la famille de brevet(s)	Date de publication
EP 0792044 A	27-08-1997	JP 10247905 A	14-09-1998
		US 5987134 A	16-11-1999
WO 9633567 A	24-10-1996	FR 2733378 A	25-10-1996
		FR 2733379 A	25-10-1996
		EP 0766894 A	09-04-1996
		JP 10506727 T	30-06-1998
		US 5910989 A	08-06-1999
WO 8911706 A	30-11-1989	AU 622915 B	30-04-1992
		AU 3733589 A	12-12-1989
		CA 1321649 A	24-08-1993
		EP 0374225 A	27-06-1990
		JP 2504435 T	13-12-1990
		US 4935962 A	19-06-1990
EP 0311470 A	12-04-1989	FR 2620248 A	10-03-1989
		AT 83573 T	15-01-1993
		AU 2197188 A	23-03-1989
		CA 1295706 A	11-02-1992
		DE 3876741 A	28-01-1993
		FI 884082 A,B,	08-03-1989
		JP 1133092 A	25-05-1989
		KR 9608209 B	20-06-1996
		US 5218637 A	08-06-1993
		US 5140634 A	18-08-1992

INTERNATIONAL SEARCH REPORT

International Application No
P[redacted]R 00/00188

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 H04L9/32

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 H04L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X A	EP 0 792 044 A (FUJI XEROX CO LTD) 27 August 1997 (1997-08-27) column 9, line 39 -column 12, line 38 figure 3	1,9,17, 22 2,10,18, 23
A	WO 96 33567 A (GEMPLUS CARD INT ;NACCACHE DAVID (FR)) 24 October 1996 (1996-10-24) page 2, line 27 -page 4, line 12 page 15, line 31 -page 18, line 17	3,4,11, 12,19, 20,24
A	WO 89 11706 A (NCR CO) 30 November 1989 (1989-11-30) page 10, line 2 -page 11, line 6 page 12, line 21 -page 14, line 6	3,4,11, 12,19, 20,24

-/--

[X] Further documents are listed in the continuation of box C.

[X] Patent family members are listed in annex.

° Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
31 March 2000	19/04/2000

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL – 2280 HV Rijswijk Tel. (+31–70) 340–2040, Tx. 31 651 epo nl, Fax: (+31–70) 340–3016	Masche, C

Form PCT/ISA/210 (second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

International Application No
P[redacted]R 00/00188

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication,where appropriate, of the relevant passages	Relevant to claim No.
A	EP 0 311 470 A (TELEDIFFUSION FSE ;FRANCE ETAT (FR); PHILIPS NV (NL)) 12 April 1989 (1989-04-12) cited in the application abstract column 12, line 30 -column 13, line 55 ---	1,9,17, 22
A	QUISQUATER J -J ET AL: "FAST DECIPHERMENT ALGORITHM FOR RSA PUBLIC-KEY CRYPTOSYSTEM" ELECTRONICS LETTERS, vol. 18, no. 21, 14 October 1982 (1982-10-14), pages 905-907, XP000577331 ISSN: 0013-5194 page 906, left-hand column, line 32 - line 61 -----	1,6,9, 14,17

Form PCT/ISA/210 (continuation of second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

Information on patent family members

International Application No
P[redacted]R 00/00188

Patent document cited in search report		Publication date	Patent family member(s)		Publication date
EP 0792044	A	27-08-1997	JP	10247905 A	14-09-1998
			US	5987134 A	16-11-1999
WO 9633567	A	24-10-1996	FR	2733378 A	25-10-1996
			FR	2733379 A	25-10-1996
			EP	0766894 A	09-04-1996
			JP	10506727 T	30-06-1998
			US	5910989 A	08-06-1999
WO 8911706	A	30-11-1989	AU	622915 B	30-04-1992
			AU	3733589 A	12-12-1989
			CA	1321649 A	24-08-1993
			EP	0374225 A	27-06-1990
			JP	2504435 T	13-12-1990
			US	4935962 A	19-06-1990
EP 0311470	A	12-04-1989	FR	2620248 A	10-03-1989
			AT	83573 T	15-01-1993
			AU	2197188 A	23-03-1989
			CA	1295706 A	11-02-1992
			DE	3876741 A	28-01-1993
			FI	884082 A,B,	08-03-1989
			JP	1133092 A	25-05-1989
			KR	9608209 B	20-06-1996
			US	5218637 A	08-06-1993
			US	5140634 A	18-08-1992

TRAITE DE COOPERATION EN MATIERE DE BREVETS

09/889958

Expéditeur : L'ADMINISTRATION CHARGEE DE LA RECHERCHE INTERNATIONALE

PCT

21 AVR 2000

Destinataire

Cabinet Patrice VIDON
A l'att. de VIDON, PATRICE
Immeuble Germanium
80 Avenue des Buttes de Coësmes
F-35700 Rennes
FRANCE

NOTIFICATION DE TRANSMISSION DU RAPPORT DE RECHERCHE INTERNATIONALE OU DE LA DECLARATION

(règle 44.1 du PCT)

Référence du dossier du déposant ou du mandataire 5343ter.WO	Date d'expédition *(jour/mois/année)* 19/04/2000 **POUR SUITE A DONNER** voir les paragraphes 1 et 4 ci-après
Demande internationale n° PCT/FR 00/00188	Date du dépôt international *(jour/mois/année)* 27/01/2000
Déposant FRANCE TELECOM et al.	

1. [X] Il est notifié au déposant que le rapport de recherche internationale a été établi et lui est transmis ci-joint.

   Dépôt de modifications et d'une déclaration selon l'article 19 :
   Le déposant peut, s'il le souhaite, modifier les revendications de la demande internationale (voir la règle 46):

   Quand? Le délai dans lequel les modifications doivent être déposées est de deux mois à compter de la date de transmission du rapport de recherche internationale ; pour plus de précisions, voir cependant les notes figurant sur la feuille d'accompagnement.

   Où? Directement auprès du Bureau international de l'OMPI
   34, chemin des Colombettes
   1211 Genève 20, Suisse
   n° de télécopieur: (41-22)740.14.35

   Pour des instructions plus détaillées, voir les notes sur la feuille d'accompagnement.

2. [ ] Il est notifié au déposant qu'il ne sera pas établi de rapport de recherche internationale et la déclaration à cet effet, prévue à l'article 17.2)a), est transmise ci-joint.

3. [ ] **En ce qui concerne la réserve** pouvant être formulée, conformément à la règle 40.2, à l'égard du paiement d'une ou de plusieurs taxes additionnelles, il est notifié au déposant que

   [ ] la réserve ainsi que la décision y relative ont été transmises au Bureau international en même temps que la requête du déposant tendant à ce que le texte de la réserve et celui de la décision en question soient notifiés aux offices désignés.

   [ ] la réserve n'a encore fait l'objet d'aucune décision; dès qu'une décision aura été prise, le déposant en sera avisé.

4. **Mesure(s) consécutive(s) :** Il est rappelé au déposant ce qui suit:

   Peu après l'expiration d'un délai de **18 mois** à compter de la date de priorité, la demande internationale sera publiée par le Bureau international. Si le déposant souhaite éviter ou différer la publication, il doit faire parvenir au Bureau international une déclaration de retrait de la demande internationale, ou de la revendication de priorité, conformément aux règles 90*bis*.1 et 90*bis*.3, respectivement, avant l'achèvement de la préparation technique de la publication internationale.

   Dans un délai de **19 mois** à compter de la date de priorité, le déposant doit présenter la demande d'examen préliminaire international s'il souhaite que l'ouverture de la phase nationale soit reportée à 30 mois à compter de la date de priorité (ou même au-delà dans certains offices).

   Dans un délai de **20 mois** à compter de la date de priorité, le déposant doit accomplir les démarches prescrites pour l'ouverture de la phase nationale auprès de tous les offices désignés qui n'ont pas été élus dans la demande d'examen préliminaire international ou dans une élection ultérieure avant l'expiration d'un délai de 19 mois à compter de la date de priorité ou qui ne pouvaient pas être élus parce qu'ils ne sont pas liés par le chapitre II.

Nom et adresse postale de l'administration chargée de la recherche internationale Office Européen des Brevets, P.B. 5818 Patentlaan 2 NL-2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Fonctionnaire autorisé Hans Pettersson

(Voir les notes sur la feuille d'accompagnement)

NOTES RELATIVES AU FORMULAIRE PCT/ISA/220

Les présentes notes sont destinées à donner les instructions essentielles concernant le dépôt de modifications selon l'article 19. Les notes sont fondées sur les exigences du Traité de coopération en matière de brevets (PCT), du règlement d'exécution et des instructions administratives du PCT. En cas de divergence entre les présentes notes et ces exigences, ce sont ces dernières qui priment. Pour de plus amples renseignements, on peut aussi consulter le Guide du déposant du PCT, qui est une publication de l'OMPI.

Dans les présentes notes, les termes "article", "règle" et "instruction" renvoient aux dispositions du traité, de son règlement d'exécution et des instructions administratives du PCT, respectivement.

INSTRUCTIONS CONCERNANT LES MODIFICATIONS SELON L'ARTICLE 19

Après réception du rapport de recherche internationale, le déposant a la possibilité de modifier une fois les revendications de la demande internationale. On notera cependant que, comme toutes les parties de la demande internationale (revendications, description et dessins) peuvent être modifiées au cours de la procédure d'examen préliminaire international, il n'est généralement pas nécessaire de déposer de modifications des revendications selon l'article 19 sauf, par exemple, au cas où le déposant souhaite que ces dernières soient publiées aux fins d'une protection provisoire ou a une autre raison de modifier les revendications avant la publication internationale. En outre, il convient de rappeler que l'obtention d'une protection provisoire n'est possible que dans certains Etats.

Quelles parties de la demande internationale peuvent être modifiées?

Selon l'article 19, les revendications exclusivement.

Durant la phase internationale, les revendications peuvent aussi être modifiées (ou modifiées à nouveau) selon l'article 34 auprès de l'administration chargée de l'examen préliminaire international. La description et les dessins ne peuvent être modifiées que selon l'article 34 auprès de l'administration chargée de l'examen préliminaire international.

Lors de l'ouverture de la phase nationale, toutes les parties de la demande internationale peuvent être modifiées selon l'article 28 ou, le cas échéant, selon l'article 41.

Quand? Dans un délai de deux mois à compter de la date de transmission du rapport de recherche internationale ou de 16 mois à compter de la date de priorité, selon l'échéance la plus tardive. Il convient cependant de noter que les modifications seront réputées avoir été reçues en temps voulu si elles parviennent au Bureau international après l'expiration du délai applicable mais avant l'achèvement de la préparation technique de la publication internationale (règle 46.1).

Où ne pas déposer les modifications?

Les modifications ne peuvent être déposées qu'auprès du Bureau international; elles ne peuvent être déposées ni auprès de l'office récepteur ni auprès de l'administration chargée de la recherche internationale (règle 46.2).

Lorsqu'une demande d'examen préliminaire international a été/est déposée, voir plus loin.

Comment? Soit en supprimant entièrement une ou plusieurs revendications, soit en ajoutant une ou plusieurs revendications nouvelles ou encore en modifiant le texte d'une ou de plusieurs des revendications telles que déposées.

Une feuille de remplacement doit être remise pour chaque feuille des revendications qui, en raison d'une ou de plusieurs modifications, diffère de la feuille initialement déposée.

Toutes les revendications figurant sur une feuille de remplacement doivent être numérotées en chiffres arabes. Si une revendication est supprimée, il n'est pas obligatoire de renuméroter les autres revendications. Chaque fois que des revendications sont renumérotées, elles doivent l'être de façon continue (instruction 205.b)).

Les modifications doivent être effectuées dans la langue dans laquelle la demande internationale est publiée.

Quels documents doivent/peuvent accompagner les modifications?

Lettre (instruction 205.b)):

Les modifications doivent être accompagnées d'une lettre.

La lettre ne sera pas publiée avec la demande internationale et les revendications modifiées. Elle ne doit pas être confondue avec la "déclaration selon l'article 19.1)" (voir plus loin sous "Déclaration selon l'article 19.1)").

La lettre doit être rédigée en anglais ou en français, au choix du déposant. Cependant, si la langue de la demande internationale est l'anglais, la lettre doit être rédigée en anglais; si la langue de la demande internationale est le français, la lettre doit être rédigée en français.

La lettre doit indiquer les différences existant entre les revendications telles que déposées et les revendications telles que modifiées. Elle doit indiquer en particulier, pour chaque revendication figurant dans la demande internationale (étant entendu que des indications identiques concernant plusieurs revendications peuvent être groupées), si

i) la revendication n'est pas modifiée;

ii) la revendication est supprimée;

iii) la revendication est nouvelle;

iv) la revendication remplace une ou plusieurs revendications telles que déposées;

v) la revendication est le résultat de la division d'une revendication telle que déposée.

Les exemples suivants illustrent la manière dont les modifications doivent être expliquées dans la lettre d'accompagnement:

1. [Lorsque le nombre des revendications déposées initialement s'élevait à 48 et qu'à la suite d'une modification de certaines revendications il s'élève à 51]:
"Revendications 1 à 15 remplacées par les revendications modifiées portant les mêmes numéros; revendications 30, 33 et 36 pas modifiées; nouvelles revendications 49 à 51 ajoutées."

2. [Lorsque le nombre des revendications déposées initialement s'élevait à 15 et qu'à la suite d'une modification de toutes les revendications il s'élève à 11]:
Revendications 1 à 15 remplacées par les revendications modifiées 1 à 11."

3. [Lorsque le nombre des revendications déposées initialement s'élevait à 14 et que les modifications consistent à supprimer certaines revendications et à en ajouter de nouvelles]:
"Revendications 1 à 6 et 14 pas modifiées; revendications 7 à 13 supprimées; nouvelles revendications 15,16 et 17 ajoutées." ou
"Revendications 7 à 13 supprimées; nouvelles revendications 15, 16 et 17 ajoutées; toutes les autres revendications pas modifiées."

4. [Lorsque plusieurs sortes de modifications sont faites]:
"Revendications 1-10 pas modifiées; revendications 11 à 13, 18 et 19 supprimées; revendiations 14, 15 et 16 remplacées par la revendication modifiée 14; revendication 17 divisée en revendications modifiées 15, 16 et 17; nouvelles revendications 20 et 21 ajoutées."

"Déclaration selon l'article 19.1)" (Règle 46.4)

Les modifications peuvent être accompagnées d'une déclaration expliquant les modifications et précisant l'incidence que ces dernières peuvent avoir sur la description et sur les dessins (qui ne peuvent pas être modifiés selon l'article 19.1)).

La déclaration sera publiée avec la demande internationale et les revendications modifiées.

Elle doit être rédigée dans la langue dans laquelle la demande internationale est publiée.

Elle doit être succincte (ne pas dépasser 500 mots si elle est établie ou traduite en anglais).

Elle ne doit pas être confondue avec la lettre expliquant les différences existant entre les revendications telles que déposées et les revendications telles que modifiées, et ne la remplace pas. Elle doit figurer sur une feuille distincte et doit être munie d'un titre permettant de l'identifier comme telle, constitué de préférence des mots "Déclaration selon l'article 19.1)"

Elle ne doit contenir aucun commentaire dénigrant relatif au rapport de recherche internationale ou à la pertinence des citations que ce dernier contient. Elle ne peut se référer à des citations se rapportant à une revendication donnée et contenues dans le rapport de recherche internationale qu'en relation avec une modification de cette revendication.

Conséquence du fait qu'une demande d'examen préliminaire international ait déjà été présentée

Si, au moment du dépôt de modifications effectuées en vertu de l'article 19, une demande d'examen préliminaire international a déjà été présentée, le déposant doit de préférence, lors du dépôt des modifications auprès du Bureau international, déposer également une copie de ces modifications auprès de l'administration chargée de l'examen préliminaire international (voir la règle 62.2a), première phrase).

Conséquence au regard de la traduction de la demande internationale lors de l'ouverture de la phase nationale

L'attention du déposant est appelée sur le fait qu'il peut avoir à remettre aux offices désignés ou élus, lors de l'ouverture de la phase nationale, une traduction des revendications telles que modifiées en vertu de l'article 19 au lieu de la traduction des revendications telles que déposées ou en plus de celle-ci.

Pour plus de précisions sur les exigences de chaque office désigné ou élu, voir le volume II du Guide du déposant du PCT.

TRAITE DE COOPERATION EN MATIERE DE BREVETS

09/889958

Expéditeur: L'ADMINISTRATION CHARGEE DE L'EXAMEN PRELIMINAIRE INTERNATIONAL

18 MAI 2001

PCT

Destinataire:

VIDON, PATRICE
Cabinet Patrice VIDON
Immeuble Germanium
80 Avenue des Buttes de Coësmes
35700 Rennes
FRANCE

NOTIFICATION DE TRANSMISSION DU RAPPORT D'EXAMEN PRELIMINAIRE INTERNATIONAL
(règle 71.1 du PCT)

Date d'expédition *(jour/mois/année)*	15.05.2001
Référence du dossier du déposant ou du mandataire: 5343.WO	**NOTIFICATION IMPORTANTE**

Demande internationale No.	Date du dépot international *(jour/mois/année)*	Date de priorité *(jour/mois/année)*
PCT/FR00/00188	27/01/2000	27/01/1999

Déposant: FRANCE TELECOM et al.

1. Il est notifié au déposant que l'administration chargée de l'examen préliminaire international a établi le rapport d'examen préliminaire international pour la demande internationale et le lui transmet ci-joint, accompagné, le cas échéant, de ces annexes.

2. Une copie du présent rapport et, le cas échéant, de ses annexes est transmise au Bureau international pour communication à tous les offices élus.

3. Si tel ou tel office élu l'exige, le Bureau international établira une traduction en langue anglaise du rapport (à l'exclusion des annexes de celui-ci) et la transmettra aux offices intéressés.

4. **RAPPEL**

Pour aborder la phase nationale auprès de chaque office élu, le déposant doit accomplir certains actes (dépôt de traduction et paiement des taxes nationales) dans le délai de 30 mois à compter de la date de priorité (ou plus tard pour ce qui concerne certains offices) (article 39.1) (voir aussi le rappel envoyé par le Bureau international dans le formulaire PCT/IB/301).

Losrqu'une traduction de la demande internationale doit être remise à un office élu, elle doit comporter la traduction de toute annexe du rapport d'examen préliminaire international. Il appartient au déposant d'établir la traduction en question et de la remettre directement à chaque office élu intéressé.

Pour plus de précisions en ce qui concerne les délais applicables et les exigences des offices élus, voir le Volume II du Guide du déposant du PCT.

Nom et adresse postale de l'adminstration chargée de l'examen préliminaire international Office européen des brevets D-80298 Munich Tél. +49 89 2399 - 0 Tx: 523656 epmu d Fax: +49 89 2399 - 4465	Fonctionnaire autorisé Barrio Baranano, A Tél.+49 89 2399-8621

Formulaire PCT/IPEA/416 (juillet 1992)

TRAITE DE COOPERATION EN MATIERE DE BREVETS

PCT

RAPPORT D'EXAMEN PRELIMINAIRE INTERNATIONAL

(article 36 et règle 70 du PCT)

Référence du dossier du déposant ou du mandataire 5343.WO	**POUR SUITE A DONNER**	voir la notification de transmission du rapport d'examen préliminaire international (formulaire PCT/IPEA/416)
Demande internationale n° PCT/FR00/00188	Date du dépot international *(jour/mois/année)* 27/01/2000	Date de priorité *(jour/mois/année)* 27/01/1999
Classification internationale des brevets (CIB) ou à la fois classification nationale et CIB H04L9/32		
Déposant FRANCE TELECOM et al.		

1. Le présent rapport d'examen préliminaire international, établi par l'administaration chargée de l'examen préliminaire international, est transmis au déposant conformément à l'article 36.

2. Ce RAPPORT comprend 6 feuilles, y compris la présente feuille de couverture.

   ☒ Il est accompagné d'ANNEXES, c'est-à-dire de feuilles de la description, des revendications ou des dessins qui ont été modifiées et qui servent de base au présent rapport ou de feuilles contenant des rectifications faites auprès de l'administration chargée de l'examen préliminaire international (voir la règle 70.16 et l'instruction 607 des Instructions administratives du PCT).

   Ces annexes comprennent 28 feuilles.

3. Le présent rapport contient des indications relatives aux points suivants:

   - I ☒ Base du rapport
   - II ☐ Priorité
   - III ☐ Absence de formulation d'opinion quant à la nouveauté, l'activité inventive et la possibilité d'application industrielle
   - IV ☐ Absence d'unité de l'invention
   - V ☒ Déclaration motivée selon l'article 35(2) quant à la nouveauté, l'activité inventive et la possibilité d'application industrielle; citations et explications à l'appui de cette déclaration
   - VI ☐ Certains documents cités
   - VII ☐ Irrégularités dans la demande internationale
   - VIII ☒ Observations relatives à la demande internationale

Date de présentation de la demande d'examen préliminaire internationale	Date d'achèvement du présent rapport
19/07/2000	15.05.2001
Nom et adresse postale de l'administration chargée de l'examen préliminaire international: Office européen des brevets D-80298 Munich Tél. +49 89 2399 - 0 Tx: 523656 epmu d Fax: +49 89 2399 - 4465	Fonctionnaire autorisé Cretaine, P N° de téléphone +49 89 2399 8828

Formulaire PCT/IPEA/409 (feuille de couverture) (janvier 1994)

RAPPORT D'EXAMEN PRÉLIMINAIRE INTERNATIONAL

Demande internationale n° PCT/FR00/00188

I. Base du rapport

1. En ce qui concerne les **éléments** de la demande internationale (*les feuilles de remplacement qui ont été remises à l'office récepteur en réponse à une invitation faite conformément à l'article 14 sont considérées dans le présent rapport comme "initialement déposées" et ne sont pas jointes en annexe au rapport puisqu'elles ne contiennent pas de modifications (règles 70.16 et 70.17)*):

Description, pages:

1-52 version initiale

Revendications, N°:

1-24 reçue(s) le 10/01/2001 avec la lettre du 09/01/2001

2. En ce qui concerne la **langue**, tous les éléments indiqués ci-dessus étaient à la disposition de l'administration ou lui ont été remis dans la langue dans laquelle la demande internationale a été déposée, sauf indication contraire donnée sous ce point.

   Ces éléments étaient à la disposition de l'administration ou lui ont été remis dans la langue suivante: , qui est :

   ☐ la langue d'une traduction remise aux fins de la recherche internationale (selon la règle 23.1(b)).

   ☐ la langue de publication de la demande internationale (selon la règle 48.3(b)).

   ☐ la langue de la traduction remise aux fins de l'examen préliminaire internationale (selon la règle 55.2 ou 55.3).

3. En ce qui concerne les **séquences de nucléotides ou d'acide aminés** divulguées dans la demande internationale (le cas échéant), l'examen préliminaire internationale a été effectué sur la base du listage des séquences :

   ☐ contenu dans la demande internationale, sous forme écrite.

   ☐ déposé avec la demande internationale, sous forme déchiffrable par ordinateur.

   ☐ remis ultérieurement à l'administration, sous forme écrite.

   ☐ remis ultérieurement à l'administration, sous forme déchiffrable par ordinateur.

   ☐ La déclaration, selon laquelle le listage des séquences par écrit et fourni ultérieurement ne va pas au-delà de la divulgation faite dans la demande telle que déposée, a été fournie.

   ☐ La déclaration, selon laquelle les informations enregistrées sous déchiffrable par ordinateur sont identiques à celles du listages des séquences Présenté par écrit, a été fournie.

4. Les modifications ont entraîné l'annulation :

   ☐ de la description, pages :

   ☐ des revendications, n^{os} :

   ☐ des dessins, feuilles :

5. ☐ Le présent rapport a été formulé abstraction faite (de certaines) des modifications, qui ont été considérées comme allant au-delà de l'exposé de l'invention tel qu'il a été déposé, comme il est indiqué ci-après (règle 70.2(c)) :

   (Toute feuille de remplacement comportant des modifications de cette nature doit être indiquée au point 1 et annexée au présent rapport)

6. Observations complémentaires, le cas échéant :

V. Déclaration motivée selon l'article 35(2) quant à la nouveauté, l'activité inventive et la possibilité d'application industrielle; citations et explications à l'appui de cette déclaration

1. Déclaration

Nouveauté	Oui :	Revendications	1.24
	Non :	Revendications	
Activité inventive	Oui :	Revendications	1-24
	Non :	Revendications	
Possibilité d'application industrielle	Oui :	Revendications	1-24
	Non :	Revendications	

2. Citations et explications
   voir feuille séparée

VIII. Observations relatives à la demande internationale

Les observations suivantes sont faites au sujet de la clarté des revendications, de la description et des dessins et de la question de savoir si les revendications se fondent entièrement sur la description :
voir feuille séparée

Concernant le point V
Déclaration motivée selon l'article 35(2) quant à la nouveauté, l'activité inventive et la possibilité d'application industrielle; citations et explications à l'appui de cette déclaration

L'invention concerne un procédé (revendication 1) et un système (revendications 9 et 17) destinés à prouver à une entité contrôleur l'authenticité d'une entité et/ou l'intégrité d'un message associé à cette entité, utilisant des étapes successives de calculs d'engagement par un dispositif témoin, de réception de défis par le témoin, et de calculs de réponses par le témoin pour contrôle par le contrôleur. Elle concerne aussi un dispositif contrôleur (revendication 21) utilisant ce procédé.

Etat de la technique:

EP-A-0 311 470, cité dans la demande, décrit un tel procédé selon lequel une entité appelée "autorité de confiance" attribue une identité à chaque entité appelée "témoin" et en calcule la signature RSA; durant un processus de personnalisation, l'autorité de confiance donne identité et signature au témoin. Par suite, le témoin proclame: "Voici mon identité; j'en connais la signature RSA.". Le témoin prouve sans la révéler qu'il connaît la signature RSA de son identité. Grâce à la clé publique de vérification RSA distribuée par l'autorité de confiance, une entité appelée "contrôleur" vérifie sans en prendre connaissance que la signature RSA correspond à l'identité proclamée. Les mécanismes utilisant ce procédé se déroulent "sans transfert de connaissance": le témoin ne connaît pas la clé privée RSA avec laquelle l'autorité de confiance signe un grand nombre d'identités. Le procédé fait appel à des valeurs privées Qi et des valeurs publiques Gi liées par une équation générique $Gi.Gi^{v} = 1. \text{ mod. } n$ (v étant un exposant public).

Problème:

La charge de travail liée aux opérations arithmétiques RSA entraîne des temps de calculs trop importants pour les applications type carte à puce.

Invention:

Le procédé n'utilise pas la signature RSA et calcule des engagements R, défis d et réponses R à partir de valeurs publiques /privées G_i et Q_i définis selon les caractéristiques de la revendication 1.
Aucun des documents cités dans le rapport de recherche international ne divulgue ou suggère les étapes de calcul définies dans la revendication 1. En particulier, EP-A-0 792 044 (cat. X) se rapporte aussi à un procédé d'authentification par défi/réponse, mais utilisant la technologie RSA.
L'objet de la revendication 1 implique par conséquent une activité inventive (article 33 PCT).

Les revendications indépendantes 9 et 17 correspondent à la revendication 1 en termes de systèmes comportant le dispositif témoin calculant les engagements, recevant les défis et calculant les réponses. Elles remplissent donc aussi les conditions de l'article 33 PCT.

La revendication indépendante 21 est relative à un dispositif contrôleur utilisant les calculs de G_i et Q_i propres au procédé de l'invention. Ces calculs n'étant ni divulgués ni suggérés par les documents cités, cette revendication remplit aussi les conditions de l'article 33 PCT.

Les autres revendications sont dépendantes et satisfont donc également, en tant que telles, aux conditions requises par le PCT en ce qui concerne la nouveauté et l'activité inventive.

Concernant le point VIII
Observations relatives à la demande internationale

Les revendications suivantes ne remplissent pas entièrement les conditions de l'article 6 PCT relatives à la clarté pour les raisons suivantes:

1. revendication indépendante 1:

   L'étape de contrôle par l'entité "contrôleur" n'étant pas indiquée dans la revendication, la désignation de l'objet de l'invention ("procédé destiné à prouver à une entité contrôleur l'authenticité d'une entité et/ou l'intégrité d'un message") n'est pas claire, les caractéristiques énoncées dans la revendication se rapportant uniquement aux calculs des valeurs d'engagements/défis/réponses utilisables dans le procédé d'authentification selon l'invention.

2. Les revendications indépendantes 9 et 17 contiennent les mêmes caractéristiques que la revendication 1 mais exprimées respectivement en terme de système et de dispositif terminal comportant le dispositif témoin calculant des engagements et des réponses à des défis reçus. L' objection mentionnée au paragraphe 1 ci-dessus est donc aussi valables pour ces revendications.

3. La revendication indépendante 21 se rapporte à un dispositif contrôleur destiné à coopérer avec le dispositif terminal ou témoin. Elle ne comporte cependant aucune caractéristique de dispositif ou système mais des caractéristiques de méthode ou procédé, dont certaines sont de plus des caractéristiques extérieures au système revendiqué ("inconnus du dispositif contrôleur"). De plus cette revendication ne comportent pas les moyens de production de défi qui sont nécessaires au processus d'authentification décrit dans la description dans son ensemble. La revendication indépendante 21 ne remplit donc pas la condition visée à l'article 6 PCT en combinaison avec la règle 6.3 b) PCT, qui prévoient qu'une revendication indépendante doit contenir toutes les caractéristiques techniques essentielles à la définition de l'invention.

Revendications

Revendications

1. Procédé destiné à prouver à une entité contrôleur,

- l'authenticité d'une entité et/ou
- l'intégrité d'un message **M** associé à cette entité,

au moyen:

- de **m** couples de valeurs privées $Q_1, Q_2, \ldots Q_m$ et publiques $G_1, G_2, \ldots G_m$, **m** étant supérieur ou égal à 1, ou des paramètres dérivés de ceux-ci,
- d'un module public **n** constitué par le produit de **f** facteurs premiers $p_1, p_2, \ldots p_f$, **f** étant supérieur ou égal à 2 ;

ledit module et lesdites valeurs étant liés par des relations du type :

$$G_i \cdot Q_i^v \equiv 1 \cdot \mathbf{mod}\ n \text{ ou } G_i \equiv Q_i^v \mathbf{mod}\ n ;$$

v désignant un exposant public ;

ledit procédé met en œuvre selon les étapes suivantes une entité appelée témoin disposant des **f** facteurs premiers p_i et/ou des paramètres des restes chinois des facteurs premiers et/ou du module public **n** et/ou des **m** valeurs privées Q_i et/ou des **f.m** composantes $Q_{i,j}$ ($Q_{i,j} \equiv Q_i \mathbf{mod}\ p_j$) des valeurs privées Q_i et de l'exposant public **v** ;

- le témoin calcule des engagements **R** dans l'anneau des entiers modulo **n** ; chaque engagement étant calculé en effectuant des opérations du type

$$R_i \equiv r_i^v \mathbf{mod}\ p_i$$

où r_i est un aléa associé au nombre premier p_i tel que $0 < r_i < p_i$, chaque r_i appartenant à une collection d'aléas $\{r_1, r_2, \ldots r_f\}$, puis en appliquant la méthode des restes chinois,

- le témoin reçoit un ou plusieurs défis **d** ; chaque défi **d** comportant **m** entiers d_i ci-après appelés défis élémentaires ; le témoin calcule à partir de chaque défi **d** une réponse **D** en effectuant des opérations du type :

$$D_i \equiv r_i \cdot Q_{i,1}^{\ d1} \cdot Q_{i,2}^{\ d2} \cdot \ldots Q_{i,m}^{\ dm} \mathbf{mod}\ p_i$$

puis en appliquant la méthode des restes chinois ;

ledit procédé étant tel qu'il y a autant de réponses **D** que de défis **d** que d'engagements **R**, chaque groupe de nombres **R, d, D** constituant un triplet noté **{R, d, D}**.

2. Procédé selon la revendication 1 destiné à prouver l'authenticité d'une entité appelée démonstrateur à une entité appelée contrôleur, ladite entité démonstrateur comprenant le témoin ;

lesdites entités démonstrateur et contrôleur exécutant les étapes suivantes :

- **étape 1 : acte d'engagement R**

- à chaque appel, le témoin calcule chaque engagement **R** en appliquant le processus spécifié selon la revendication 1,

- le démonstrateur transmet au contrôleur tout ou partie de chaque engagement **R**,

- **étape 2 : acte de défi d**

- le contrôleur, après avoir reçu tout ou partie de chaque engagement **R**, produit des défis **d** en nombre égal au nombre d'engagements **R** et transmet les défis **d** au démonstrateur,

- **étape 3 : acte de réponse D**

- le témoin calcule des réponses **D** à partir des défis **d** en appliquant le processus spécifié selon la revendication 1,

- **étape 4 : acte de contrôle**

- le démonstrateur transmet chaque réponse **D** au contrôleur,

cas où le démonstrateur a transmis une partie de chaque engagement R

dans le cas où le démonstrateur a transmis une partie de chaque engagement **R**, le contrôleur, disposant des **m** valeurs publiques G_1, G_2, ... G_m, calcule à partir de chaque défi **d** et de chaque réponse **D** un engagement reconstruit **R'** satisfaisant à une relation du type :

$$R' \equiv G_1^{d1} . G_2^{d2} . \ldots G_m^{dm} . D^v \bmod n$$

ou à une relation du type,

$$R' \equiv D^v / G_1^{d1} . G_2^{d2} . \ldots G_m^{dm} . \mathbf{mod\ n},$$

le contrôleur vérifie que chaque engagement reconstruit **R'** reproduit tout ou partie de chaque engagement **R** qui lui a été transmis,

cas où le démonstrateur a transmis l'intégralité de chaque engagement R

dans le cas où le démonstrateur a transmis l'intégralité de chaque engagement **R**, le contrôleur, disposant des **m** valeurs publiques G_1, G_2, ... G_m, vérifie que chaque engagement **R** satisfait à une relation du type :

$$R \equiv G_1^{d1} . G_2^{d2} . \ldots G_m^{dm} . D^v \mathbf{\ mod\ n}$$

ou à une relation du type,

$$R \equiv D^v / G_1^{d1} . G_2^{d2} . \ldots G_m^{dm} . \mathbf{mod\ n}.$$

3. Procédé selon la revendication 1 destiné à prouver à une entité appelée contrôleur l'intégrité d'un message **M** associé à une entité appelée démonstrateur, ladite entité démonstrateur comprenant le témoin ;

lesdites entités démonstrateur et contrôleur exécutant les étapes suivantes :

- **étape 1 : acte d'engagement R**

- à chaque appel, le témoin calcule chaque engagement **R** en appliquant le processus spécifié selon la revendication 1,

- **étape 2 : acte de défi d**

- le démonstrateur applique une fonction de hachage **h** ayant comme arguments le message **M** et tout ou partie de chaque engagement **R** pour calculer au moins un jeton **T**,

- le démonstrateur transmet le jeton **T** au contrôleur,

- le contrôleur, après avoir reçu un jeton **T**, produit des défis **d** en nombre égal au nombre d'engagements **R** et transmet les défis **d** au démonstrateur,

- **étape 3 : acte de réponse D**

- le témoin calcule des réponses **D** à partir des défis **d** en appliquant le processus spécifié selon la revendication 1,

- **étape 4 : acte de contrôle**

- le démonstrateur transmet chaque réponse **D** au contrôleur,
- le contrôleur, disposant des m valeurs publiques G_1, G_2, ... G_m, calcule à partir de chaque défi **d** et de chaque réponse **D** un engagement reconstruit **R'** satisfaisant à une relation du type :

$$R' \equiv G_1^{d1} . G_2^{d2} . \ldots G_m^{dm} . D^v \bmod n$$

ou à une relation du type :

$$R' \equiv D^v / G_1^{d1} . G_2^{d2} . \ldots G_m^{dm} . \bmod n$$

- puis le contrôleur applique la fonction de hachage **h** ayant comme arguments le message **M** et tout ou partie de chaque engagement reconstruit **R'** pour reconstruire le jeton **T'**,
- puis le contrôleur vérifie que le jeton **T'** est identique au jeton **T** transmis.

4. Procédé selon la revendication 1 destiné à produire la signature numérique d'un message **M** par une entité appelée entité signataire, ladite entité signataire comprenant le témoin ;

ladite entité signataire exécute une opération de signature en vue d'obtenir un message signé comprenant :

- le message **M**,
- les défis **d** et/ou les engagements **R**,
- les réponses **D** ;

ladite entité signataire exécute l'opération de signature en mettant en oeuvre les étapes suivantes :

- **étape 1 : acte d'engagement R**

- à chaque appel, le témoin calcule chaque engagement **R** en appliquant le processus spécifié selon la revendication 1,

- **étape 2 : acte de défi d**

- le signataire applique une fonction de hachage **h** ayant comme arguments le message **M** et chaque engagement **R** pour obtenir un train binaire,
- le signataire extrait de ce train binaire des défis **d** en nombre égal au nombre d'engagements **R**,

• étape 3 : acte de réponse D

- le témoin calcule des réponses **D** à partir des défis **d** en appliquant le processus spécifié selon la revendication 1.

5. Procédé selon la revendication 4 destiné à prouver l'authenticité du message **M** en contrôlant, par une entité appelée contrôleur, le message signé;

ladite entité contrôleur disposant du message signé exécute une opération de contrôle en procédant comme suit :

• cas où le contrôleur dispose des engagements R, des défis d, des réponses D,

dans le cas où le contrôleur dispose des engagements **R**, des défis **d**, des réponses **D**,

• • le contrôleur vérifie que les engagements **R**, les défis **d** et les réponses **D** satisfont à des relations du type

$$\mathbf{R \equiv G_1^{\,d1} . G_2^{\,d2} . \ldots G_m^{\,dm} . D^v \bmod n}$$

ou à des relations du type :

$$\mathbf{R \equiv D^v / G_1^{\,d1} . G_2^{\,d2} . \ldots G_m^{\,dm} . \bmod n}$$

• • le contrôleur vérifie que le message **M**, les défis **d** et les engagements **R** satisfont à la fonction de hachage

$$\mathbf{d = h\,(M, R)}$$

• cas où le contrôleur dispose des défis d et des réponses D

dans le cas où le contrôleur dispose des défis **d** et des réponses **D**,

• • le contrôleur reconstruit, à partir de chaque défi **d** et de chaque réponse **D**, des engagements **R'** satisfaisant à des relations du type :

$$\mathbf{R' \equiv G_1^{\,d1} . G_2^{\,d2} . \ldots G_m^{\,dm} . D^v \bmod n}$$

ou à des relations du type :

$$\mathbf{R' \equiv D^v / G_1^{\,d1} . G_2^{\,d2} . \ldots G_m^{\,dm} . \bmod n}$$

• • le contrôleur vérifie que le message **M** et les défis **d** satisfont à la fonction de hachage

$$d = h(M, R')$$

• **cas où le contrôleur dispose des engagements R et des réponses D**

dans le cas où le contrôleur dispose des engagements **R** et des réponses **D**,

• • le contrôleur applique la fonction de hachage et reconstruit **d'**

$$d' = h(M, R)$$

• • le contrôleur vérifie que les engagements **R**, les défis **d'** et les réponses **D**, satisfont à des relations du type :

$$R \equiv G_1^{d'1} . G_2^{d'2} . \ldots G_m^{d'm} . D^v \bmod n$$

ou à des relations du type :

$$R \equiv D^v / G_1^{d'1} . G_2^{d'2} . \ldots G_m^{d'm} . \bmod n$$

6. Procédé selon l'une quelconque des revendications 1 à 5 tel que les composantes $Q_{i,1}, Q_{i,2}, \ldots Q_{i,f}$ des valeurs privées Q_i, sont des nombres tirés au hasard à raison d'une composante $Q_{i,j}$ ($Q_{i,j} \equiv Q_i \bmod p_j$) pour chacun desdits facteurs premiers p_j, lesdites valeurs privées Q_i pouvant être calculées à partir desdites composantes $Q_{i,1}$, $Q_{i,2}$ ... $Q_{i,f}$ par la méthode des restes chinois,

lesdites valeurs publiques G_i, étant calculées

• en effectuant des opérations du type

$$G_{i,j} \equiv Q_{i,j}^v \bmod p_j$$

• puis en appliquant la méthode des restes chinois pour établir G_i tel que

$$G_i . Q_i^v \equiv 1 . \bmod n \text{ ou } G_i \equiv Q_i^{-v} \bmod n ;$$

7. Procédé selon la revendication 6 tel que l'exposant public de vérification **v** est un nombre premier,

8. Procédé selon l'une quelconque des revendications 1 à 5

ledit exposant **v** étant tel que

$$v = 2^k$$

où **k** est un paramètre de sécurité plus grand que 1 ;

ladite valeur publique G_i étant le carré g_i^2 d'un nombre de base g_i inférieur aux **f** facteurs premiers $p_1, p_2, \ldots p_f$; le nombre de base g_i étant tel que les

conditions suivantes sont satisfaites:

aucune des deux équations :

$$x^2 \equiv g_i \bmod n \qquad \text{et} \qquad x^2 \equiv -g_i \bmod n$$

n'a de solution en x dans l'anneau des entiers modulo **n**

et tel que l'équation :

$$x^v \equiv g_i^2 \bmod n$$

a des solutions en x dans l'anneau des entiers modulo **n** .

9. Système destiné à prouver à un serveur contrôleur,

- l'authenticité d'une entité et/ou
- l'intégrité d'un message **M** associé à cette entité,

au moyen:

- de **m** couples de valeurs privées $Q_1, Q_2, \ldots Q_m$ et publiques $G_1, G_2, \ldots G_m$, **m** étant supérieur ou égal à 1, ou des paramètres dérivés de ceux-ci,
- d'un module public **n** constitué par le produit de **f** facteurs premiers $p_1, p_2, \ldots p_f$, **f** étant supérieur ou égal à 2 ;

ledit module et lesdites valeurs étant liés par des relations du type :

$$G_i . Q_i^v \equiv 1 \bmod n \text{ ou } G_i \equiv Q_i^v \bmod n ;$$

v désignant un exposant public ;

ledit système comprend un dispositif témoin, notamment contenu dans un objet nomade se présentant par exemple sous la forme d'une carte bancaire à microprocesseur,

le dispositif témoin comporte une zone mémoire contenant les **f** facteurs premiers p_i et/ou des paramètres des restes chinois des facteurs premiers et/ou du module public **n** et/ou des **m** valeurs privées Q_i et/ou des **fm** composantes $Q_{i,j}$ ($Q_{i,j} \equiv Q_i \bmod p_j$) des valeurs privées Q_i et de l'exposant public **v** ;

le dispositif témoin comporte aussi :

- des moyens de production d'aléas, ci-après désignés les moyens de production d'aléas du dispositif témoin,

- des moyens de calcul, ci-après désignés les moyens de calcul des engagements **R** du dispositif témoin, pour calculer des engagements **R** dans l'anneau des entiers modulo **n** ; chaque engagement étant calculé en effectuant des opérations du type

$$R_i \equiv r_i^{v} \bmod p_i$$

où r_i est un aléa associé au nombre premier p_i tel que $0 < r_i < p_i$, chaque r_i appartenant à une collection d'aléas $\{r_1 , r_2 , \ldots r_f\}$ produits par les moyens de production d'aléas, puis en appliquant la méthode des restes chinois ;

le dispositif témoin comporte aussi :

- des moyens de réception, ci-après désignés les moyens de réception des défis **d** du dispositif témoin, pour recevoir un ou plusieurs défis **d** ; chaque défi **d** comportant **m** entiers d_i ci-après appelés défis élémentaires ;

- des moyens de calcul, ci-après désignés les moyens de calcul des réponses **D** du dispositif témoin, pour calculer à partir de chaque défi **d** une réponse **D** en effectuant des opérations du type :

$$D_i \equiv r_i \cdot Q_{i,1}^{\,d1} \cdot Q_{i,2}^{\,d2} \cdot \ldots Q_{i,m}^{\,dm} \bmod p_i$$

puis, en appliquant la méthode des restes chinois ;

- des moyens de transmission pour transmettre un ou plusieurs engagements **R** et une ou plusieurs réponses **D** ;

il y a autant de réponses **D** que de défis **d** que d'engagements **R**, chaque groupe de nombres **R, d, D** constituant un triplet noté **{R, d, D}**.

10. Système selon la revendication 9 destiné à prouver l'authenticité d'une entité appelée démonstrateur à une entité appelée contrôleur ;
ledit système étant tel qu'il comporte

- un dispositif démonstrateur associé à l'entité démonstrateur, ledit dispositif démonstrateur étant interconnecté au dispositif témoin par des moyens d'interconnexion et pouvant se présenter notamment sous la

forme de microcircuits logiques dans un objet nomade par exemple sous la forme d'un microprocesseur dans une carte bancaire à microprocesseur,

- un dispositif contrôleur associé à l'entité contrôleur ; ledit dispositif contrôleur se présentant notamment sous la forme d'un terminal ou d'un serveur distant ; ledit dispositif contrôleur comportant des moyens de connexion pour le connecter électriquement, électromagnétiquement, optiquement ou de manière acoustique, notamment via un réseau de communication informatique, au dispositif démonstrateur ;

ledit système permettant d'exécuter les étapes suivantes :

• **étape 1 : acte d'engagement R**

- à chaque appel, les moyens de calcul des engagements **R** du dispositif témoin calculent chaque engagement **R** en appliquant le processus spécifié selon la revendication 9,

- le dispositif témoin comporte des moyens de transmission, ci-après désignés les moyens de transmission du dispositif témoin, pour transmettre tout ou partie de chaque engagement **R** au dispositif démonstrateur, via les moyens d'interconnexion ;

- le dispositif démonstrateur comporte aussi des moyens de transmission, ci-après désigné les moyens de transmission du dispositif démonstrateur, pour transmettre tout ou partie de chaque engagement **R** au dispositif contrôleur, via les moyens de connexion ;

• **étape 2 : acte de défi d**

le dispositif contrôleur comporte des moyens de productions de défis pour produire, après avoir reçu tout ou partie de chaque engagement **R**, des défis **d** en nombre égal au nombre d'engagements **R**,

le dispositif contrôleur comporte aussi des moyens de transmission, ci-après désignés les moyens de transmission du contrôleur, pour transmettre les défis **d** au démonstrateur,

• **étape 3 : acte de réponse D**

les moyens de réception des défis **d** du dispositif témoin, reçoivent chaque défi **d** provenant du dispositif démonstrateur, via les moyens d'interconnexion,

les moyens de calcul des réponses **D** du dispositif témoin calculent les réponses **D** à partir des défis **d** en appliquant le processus spécifié selon la revendication 9,

- **étape 4 : acte de contrôle**

les moyens de transmission du démonstrateur transmettent chaque réponse **D** au contrôleur

le dispositif contrôleur comporte aussi

- des moyens de calcul, ci-après désignés les moyens de calcul du dispositif contrôleur,

- des moyens de comparaison, ci-après désignés les moyens de comparaison du dispositif contrôleur,

cas où le démonstrateur a transmis une partie de chaque engagement R

dans le cas où les moyens de transmission du démonstrateur ont transmis une partie de chaque engagement **R**, les moyens de calcul du dispositif contrôleur, disposant des **m** valeurs publiques G_1, G_2, ... G_m, calculent à partir de chaque défi **d** et de chaque réponse **D** un engagement reconstruit **R'** satisfaisant à une relation du type :

$$R' \equiv G_1^{d1} . G_2^{d2} . \ldots G_m^{dm} . D^v \bmod n$$

ou à une relation du type,

$$R' \equiv D^v / G_1^{d1} . G_2^{d2} . \ldots G_m^{dm} . \bmod n ,$$

les moyens de comparaison du dispositif contrôleur comparent chaque engagement reconstruit **R'** à tout ou partie de chaque engagement **R** reçus,

cas où le démonstrateur a transmis l'intégralité de chaque engagement R

dans le cas où les moyens de transmission du démonstrateur ont transmis l'intégralité de chaque engagement **R**, les moyens de calcul et les moyens

de comparaison du dispositif contrôleur, disposant des **m** valeurs publiques $G_1, G_2, \ldots G_m$, vérifient que chaque engagement **R** satisfait à une relation du type :

$$R \equiv G_1^{d1} . G_2^{d2} . \ldots G_m^{dm} . D^v \bmod n$$

ou à une relation du type,

$$R \equiv D^v / G_1^{d1} . G_2^{d2} . \ldots G_m^{dm} . \bmod n .$$

11. Système selon la revendication 9 destiné à prouver à une entité appelée contrôleur l'intégrité d'un message **M** associé à une entité appelée démonstrateur,

ledit système étant tel qu'il comporte

- un dispositif démonstrateur associé à l'entité démonstrateur, ledit dispositif démonstrateur étant interconnecté au dispositif témoin par des moyens d'interconnexion et pouvant se présenter notamment sous la forme de microcircuits logiques dans un objet nomade par exemple sous la forme d'un microprocesseur dans une carte bancaire à microprocesseur,

- un dispositif contrôleur associé à l'entité contrôleur ; ledit dispositif contrôleur se présentant notamment sous la forme d'un terminal ou d'un serveur distant ; ledit dispositif contrôleur comportant des moyens de connexion pour le connecter électriquement, électromagnétiquement, optiquement ou de manière acoustique, notamment via un réseau de communication informatique, au dispositif démonstrateur ;

ledit système permettant d'exécuter les étapes suivantes :

- **étape 1 : acte d'engagement R**

- à chaque appel, les moyens de calcul des engagements **R** du dispositif témoin calculent chaque engagement **R** en appliquant le processus spécifié selon la revendication 9,

- le dispositif témoin comporte des moyens de transmission, ci-après désignés les moyens de transmission du dispositif témoin, pour transmettre tout ou partie de chaque engagement **R** au dispositif démonstrateur, via les

moyens d'interconnexion ;

• **étape 2 : acte de défi d**

le dispositif démonstrateur comporte des moyens de calcul, ci-après désignés les moyens de calcul du dispositif démonstrateur, appliquant fonction de hachage **h** ayant comme arguments le message **M** et tout ou partie de chaque engagement **R** pour calculer au moins un jeton **T**,

le dispositif démonstrateur comporte aussi des moyens de transmission, ci-après désignés les moyens de transmission du démonstrateur, pour transmettre chaque jeton **T** , via les moyens de connexion, au dispositif au contrôleur,

le dispositif contrôleur comporte aussi des moyens de productions de défis pour produire, après avoir reçu le jeton **T,** les défis **d** en nombre égal au nombre d'engagements **R ,**

le dispositif contrôleur comporte aussi des moyens de transmission, ci-après désignés les moyens de transmission du dispositif contrôleur, pour transmettre les défis **d** au démonstrateur,

• **étape 3 : acte de réponse D**

les moyens de réception des défis **d** du dispositif témoin, reçoivent chaque défi **d** provenant du dispositif démonstrateur, via les moyens d'interconnexion,

les moyens de calcul des réponses **D** du dispositif témoin calculent les réponses **D** à partir des défis **d** en appliquant le processus spécifié selon la revendication 9,

• **étape 4 : acte de contrôle**

les moyens de transmission du démonstrateur transmettent chaque réponse **D** au contrôleur,

le dispositif contrôleur comporte aussi des moyens de calcul, ci-après désignés les moyens de calcul du dispositif contrôleur, disposant des **m** valeurs publiques G_1, G_2, ... G_m, pour d'une part, calculer à partir de

chaque défi **d** et de chaque réponse **D** un engagement reconstruit **R'** satisfaisant à une relation du type :

$$R' \equiv G_1^{d1} . G_2^{d2} . \ldots G_m^{dm} . D^v \bmod n$$

ou à une relation du type :

$$R' \equiv D^v / G_1^{d1} . G_2^{d2} . \ldots G_m^{dm} . \bmod n$$

puis d'autre part, calculer en appliquant la fonction de hachage **h** ayant comme arguments le message **M** et tout ou partie de chaque engagement reconstruit **R'**, un jeton **T'**,

le dispositif contrôleur comporte aussi des moyens de comparaison, ci-après désignés les moyens de comparaison du dispositif contrôleur, pour comparer le jeton **T'** au jeton **T** reçu.

12. Système selon la revendication 9 destiné à produire la signature numérique d'un message **M**, ci après désigné le message signé, par une entité appelée entité signataire,

le message signé comprenant :

- le message **M**,
- les défis **d** et/ou les engagements **R**,
- les réponses **D** ;

ledit système étant tel qu'il comporte un dispositif signataire associé à l'entité signataire, ledit dispositif signataire étant interconnecté au dispositif témoin par des moyens d'interconnexion et pouvant se présenter notamment sous la forme de microcircuits logiques dans un objet nomade par exemple sous la forme d'un microprocesseur dans une carte bancaire à microprocesseur,

ledit système permettant d'exécuter les étapes suivantes :

- **étape 1 : acte d'engagement R**

à chaque appel, les moyens de calcul des engagements **R** du dispositif témoin calculent chaque engagement **R** en appliquant le processus spécifié selon la revendication 9,

le dispositif témoin comporte des moyens de transmission, ci-après désignés les moyens de transmission du dispositif témoin, pour transmettre tout ou partie de chaque engagement **R** au dispositif signataire, via les moyens d'interconnexion;

- **étape 2 : acte de défi d**

le dispositif signataire comporte des moyens de calcul, ci-après désignés les moyens de calcul du dispositif signataire, appliquant une fonction d hachage **h** ayant comme arguments le message **M** et chaque engagement **R** pour calculer un train binaire et extraire de ce train binaire des défis **d** en nombre égal au nombre d'engagements **R,**

- **étape 3 : acte de réponse D**

les moyens de réception des défis **d** , reçoivent chaque défi **d** provenant du dispositif signataire, via les moyens d'interconnexion,

les moyens de calcul des réponses **D** du dispositif témoin calculent les réponses **D** à partir des défis **d** en appliquant le processus spécifié selon la revendication 9,

le dispositif témoin comporte des moyens de transmission, ci-après désignés les moyens de transmission du dispositif témoin, pour transmettre les réponses **D** au dispositif signataire, via les moyens d'interconnexion.

13. Système selon la revendication 11 destiné à prouver l'authenticité du message **M** en contrôlant, par une entité appelée contrôleur, le message signé;

ledit système étant tel qu'il comporte un dispositif contrôleur associé à l'entité contrôleur ; ledit dispositif contrôleur se présentant notamment sous la forme d'un terminal ou d'un serveur distant ; ledit dispositif contrôleur comportant des moyens de connexion pour le connecter électriquement, électromagnétiquement, optiquement ou de manière acoustique, notamment via un réseau de communication informatique, au dispositif signataire ;

ledit dispositif signataire associé à l'entité signataire comporte des moyens de transmission, ci-après désignés les moyens de transmission du dispositif signataire, pour transmettre au dispositif contrôleur, le message signé, via les moyens de connexion, de telle sorte que le dispositif contrôleur dispose d'un message signé comprenant:

- le message **M**,
- les défis **d** et/ou les engagements **R**,
- les réponse **D**

le dispositif contrôleur comporte :

- des moyens de calcul, ci-après désignés les moyens de calcul du dispositif contrôleur,
- des moyens de comparaison, ci-après désignés les moyens de comparaison du dispositif contrôleur,

• cas où le contrôleur dispose des engagements R, des défis d, des réponses D,

dans le cas où le dispositif contrôleur dispose des engagements **R**, des défis **d**, des réponses **D**,

• • les moyens de calcul et de comparaison du dispositif contrôleur vérifient que les engagements **R**, les défis **d** et les réponses **D** satisfont à des relations du type

$$\mathbf{R \equiv G_1^{d1} . G_2^{d2} . \ldots G_m^{dm} . D^v \bmod n}$$

ou à des relations du type :

$$\mathbf{R \equiv D^v / G_1^{d1} . G_2^{d2} . \ldots G_m^{dm} . \bmod n}$$

• • les moyens de calcul et de comparaison du dispositif contrôleur vérifient que le message **M**, les défis **d** et les engagements **R** satisfont à la fonction de hachage

$$\mathbf{d = h\,(M, R)}$$

• cas où le contrôleur dispose des défis d et des réponses D

dans le cas où le dispositif contrôleur dispose des défis **d** et des réponses **D**,

•• les moyens de calcul du dispositif contrôleur calculent, à partir de chaque défi **d** et de chaque réponse **D**, des engagements **R'** satisfaisant à des relations du type :

$$R' \equiv G_1^{d1} . G_2^{d2} . \ldots G_m^{dm} . D^v \bmod n$$

ou à des relations du type :

$$R' \equiv D^v / G_1^{d1} . G_2^{d2} . \ldots G_m^{dm} . \bmod n$$

•• les moyens de calcul et de comparaison du dispositif contrôleur vérifie que le message **M** et les défis **d** satisfont à la fonction de hachage

$$d = h(M, R')$$

• cas où le contrôleur dispose des engagements R et des réponses D

dans le cas où le dispositif contrôleur dispose des engagements **R** et des réponses **D**,

•• les moyens de calcul du dispositif contrôleur appliquent la fonction de hachage et calculent **d'** tel que

$$d' = h(M, R)$$

•• les moyens de calcul et de comparaison du dispositif contrôleur vérifient que les engagements **R**, les défis **d'** et les réponses **D**, satisfont à des relations du type :

$$R \equiv G_1^{d'1} . G_2^{d'2} . \ldots G_m^{d'm} . D^v \bmod n$$

ou à des relations du type :

$$R \equiv D^v / G_1^{d'1} . G_2^{d'2} . \ldots G_m^{d'm} . \bmod n$$

14. Système selon l'une quelconque des revendications 9 à 13 tel que les composantes $Q_{i,1}$, $Q_{i,2}$, ... $Q_{i,f}$ des valeurs privées Q_i, sont des nombres tirés au hasard à raison d'une composante $Q_{i,j}$ ($Q_{i,j} \equiv Q_i \bmod p_j$) pour chacun desdits facteurs premiers p_j, lesdites valeurs privées Q_i pouvant être calculées à partir desdites composantes $Q_{i,1}$, $Q_{i,2}$ ... $Q_{i,f}$ par la méthode des restes chinois,

lesdites valeurs publiques G_j, étant calculées

• en effectuant des opérations du type

$$G_{i,j} \equiv Q_{i,j}^{v} \bmod p_j$$

• puis en appliquant la méthode des restes chinois pour établir G_i tel que

$$G_i . Q_i^v \equiv 1 . \bmod n \text{ ou } G_i \equiv Q_i^v \bmod n ;$$

15. Système selon la revendication 14 tel que l'exposant public de vérification **v** est un nombre premier.

16. Système selon l'une quelconque des revendications 9 à 13 ledit exposant **v** étant tel que

$$v = 2^k$$

où **k** est un paramètre de sécurité plus grand que 1 ;

ladite valeur publique G_i étant le carré g_i^2 d'un nombre de base g_i inférieur aux f facteurs premiers $p_1, p_2, \ldots p_f$; le nombre de base g_i étant tel que les conditions suivantes sont satisfaites :

aucune deux équations :

$$x^2 \equiv g_i \bmod n \qquad \text{et} \qquad x^2 \equiv - g_i \bmod n$$

n'a de solution en x dans l'anneau des entiers modulo **n**

et tel que l'équation :

$$x^v \equiv g_i^2 \bmod n$$

a des solutions en x dans l'anneau des entiers modulo **n** .

17. Dispositif terminal associé à une entité, se présentant notamment sous la forme d'un objet nomade par exemple sous la forme d'une carte bancaire à microprocesseur, destiné à prouver à dispositif contrôleur,

- l'authenticité d'une entité et/ou
- l'intégrité d'un message M associé à cette entité,

au moyen:

- de **m** couples de valeurs privées $Q_1, Q_2, \ldots Q_m$ et publiques $G_1, G_2, \ldots G_m$, **m** étant supérieur ou égal à 1,
- d'un module public **n** constitué par le produit de **f** facteurs premiers $p_1, p_2, \ldots p_f$, f étant supérieur ou égal à 2 ;

ledit module et lesdites valeurs étant liés par des relations du type :

$$G_i \cdot Q_i^v \equiv 1 \cdot \mathbf{mod}\ n \text{ ou } G_i \equiv Q_i^v \mathbf{mod}\ n ;$$

v désignant un exposant public ;

ledit dispositif terminal comprend un dispositif témoin comportant une zone mémoire contenant les **f** facteurs premiers p_i et/ou des paramètres des restes chinois des facteurs premiers et/ou du module public **n** et/ou des **m** valeurs privées Q_i et/ou des **f.m** composantes $Q_{i,j}$ ($Q_{i,j} \equiv Q_i \mathbf{mod}\ p_j$) des valeurs privées Q_i et de l'exposant public **v** ;

le dispositif témoin comporte aussi :

- des moyens de production d'aléas, ci-après désignés les moyens de production d'aléas du dispositif témoin,

- des moyens de calcul, ci-après désignés les moyens de calcul des engagements **R** du dispositif témoin, pour calculer des engagements **R** dans l'anneau des entiers modulo **n** ; chaque engagement étant calculé en effectuant des opérations du type

$$R_i \equiv r_i^v \mathbf{mod}\ p_i$$

où r_i est un aléa associé au nombre premier p_i tel que $0 < r_i < p_i$, chaque r_i appartenant à une collection d'aléas $\{r_1, r_2, \ldots r_f\}$ produits par les moyens de production d'aléas, puis en appliquant la méthode des restes chinois ;

le dispositif témoin comporte aussi :

- des moyens de réception, ci-après désignés les moyens de réception des défis **d** du dispositif témoin, pour recevoir un ou plusieurs défis **d** ; chaque défi **d** comportant **m** entiers d_i ci-après appelés défis élémentaires ;

- des moyens de calcul, ci-après désignés les moyens de calcul des réponses **D** du dispositif témoin, pour calculer à partir de chaque défi **d** une réponse **D** en effectuant des opérations du type :

$$D_i \equiv r_i \cdot Q_{i,1}^{\ d1} \cdot Q_{i,2}^{\ d2} \cdot \ldots Q_{i,m}^{\ dm} \mathbf{mod}\ p_i$$

puis, en appliquant la méthode des restes chinois ;

- des moyens de transmission pour transmettre un ou plusieurs engagements **R** et une ou plusieurs réponses **D** ;

il y a autant de réponses **D** que de défis **d** que d'engagements **R**, chaque groupe de nombres **R, d, D** constituant un triplet noté **{R, d, D}**.

18. Dispositif terminal selon la revendication 17 destiné à prouver l'authenticité d'une entité appelée démonstrateur à une entité appelée contrôleur ;

ledit dispositif terminal étant tel qu'il comporte un dispositif démonstrateur associé à l'entité démonstrateur, ledit dispositif démonstrateur étant interconnecté au dispositif témoin par des moyens d'interconnexion et pouvant se présenter notamment sous la forme de microcircuits logiques dans un objet nomade par exemple sous la forme d'un microprocesseur dans une carte bancaire à microprocesseur,

ledit dispositif démonstrateur comportant des moyens de connexion pour le connecter électriquement, électromagnétiquement, optiquement ou de manière acoustique, notamment via un réseau de communication informatique, à un dispositif contrôleur associé à l'entité contrôleur ; ledit dispositif contrôleur se présentant notamment sous la forme d'un terminal ou d'un serveur distant ;

ledit dispositif terminal permettant d'exécuter les étapes suivantes :

- **étape 1 : acte d'engagement R**

- à chaque appel, les moyens de calcul des engagements **R** du dispositif témoin calculent chaque engagement **R** en appliquant le processus spécifié selon la revendication 17,

- le dispositif témoin comporte des moyens de transmission, ci-après désignés les moyens de transmission du dispositif témoin, pour transmettre tout ou partie de chaque engagement **R** au dispositif démonstrateur, via les moyens d'interconnexion ;

le dispositif démonstrateur comporte aussi des moyens de transmission, ci-

après désignés les moyens de transmission du démonstrateur, pour transmettre tout ou partie de chaque engagement **R** au dispositif contrôleur, via les moyens de connexion,

• **étape 2 et 3 : acte de défi d, acte de réponse D**

les moyens de réception des défis **d** du dispositif témoin, reçoivent chaque défi **d** provenant du dispositif contrôleur via les moyens de connexion entre le dispositif contrôleur et le dispositif démonstrateur et via les moyens d'interconnexion entre le dispositif démonstrateur et le dispositif témoin,

les moyens de calcul des réponses **D** du dispositif témoin calculent les réponses **D** à partir des défis **d** en appliquant le processus spécifié selon la revendication 17,

• **étape 4 : acte de contrôle**

les moyens de transmission du démonstrateur transmettent chaque réponse **D** au dispositif contrôleur qui procède au contrôle.

19. Dispositif terminal selon la revendication 17 destiné à prouver à une entité appelée contrôleur l'intégrité d'un message **M** associé à une entité appelée démonstrateur,

ledit dispositif terminal étant tel qu'il comporte un dispositif démonstrateur associé à l'entité démonstrateur, ledit dispositif démonstrateur étant interconnecté au dispositif témoin par des moyens d'interconnexion et pouvant se présenter notamment sous la forme de microcircuits logiques dans un objet nomade par exemple sous la forme d'un microprocesseur dans une carte bancaire à microprocesseur,

ledit dispositif démonstrateur comportant des moyens de connexion pour le connecter électriquement, électromagnétiquement, optiquement ou de manière acoustique, notamment via un réseau de communication informatique, à un dispositif contrôleur associé à l'entité contrôleur ; ledit dispositif contrôleur se présentant notamment sous la forme d'un terminal ou d'un serveur distant ;

ledit dispositif terminal permettant d'exécuter les étapes suivantes :

• **étape 1 : acte d'engagement R**

- à chaque appel, les moyens de calcul des engagements **R** du dispositif témoin calculent chaque engagement **R** en appliquant le processus spécifié selon la revendication 17,

- le dispositif témoin comporte des moyens de transmission, ci-après désignés les moyens de transmission du dispositif témoin, pour transmettre tout ou partie de chaque engagement **R** au dispositif démonstrateur, via les moyens d'interconnexion ;

• **étape 2 et 3 : acte de défi d, acte de réponse**

le dispositif démonstrateur comporte des moyens de calcul, ci-après désignés les moyens de calcul du dispositif démonstrateur, appliquant fonction de hachage **h** ayant comme arguments le message **M** et tout ou partie de chaque engagement **R** pour calculer au moins un jeton **T**,

le dispositif démonstrateur comporte aussi des moyens de transmission, ci-après désignés les moyens de transmission du démonstrateur, pour transmettre chaque jeton **T** , via les moyens de connexion, au dispositif au contrôleur,

les moyens de réception des défis **d** du dispositif témoin, reçoivent chaque défi **d** provenant du dispositif démonstrateur, via les moyens d'interconnexion,

les moyens de calcul des réponses **D** du dispositif témoin calculent les réponses **D** à partir des défis **d** en appliquant le processus spécifié selon la revendication 17,

• **étape 4 : acte de contrôle**

les moyens de transmission du démonstrateur transmettent chaque réponse **D** au dispositif contrôleur qui procède au contrôle.

20. Dispositif terminal selon la revendication 17 destiné à produire la signature numérique d'un message **M**, ci après désigné le message signé,

par une entité appelée entité signataire,

le message signé comprenant :

- le message **M**,
- les défis **d** et/ou les engagements **R**,
- les réponses **D** ;

ledit dispositif terminal étant tel qu'il comporte un dispositif signataire associé à l'entité signataire, ledit dispositif signataire étant interconnecté au dispositif témoin par des moyens d'interconnexion et pouvant se présenter notamment sous la forme de microcircuits logiques dans un objet nomade par exemple sous la forme d'un microprocesseur dans une carte bancaire à microprocesseur,

ledit dispositif signataire comportant des moyens de connexion pour le connecter électriquement, électromagnétiquement, optiquement ou de manière acoustique, notamment via un réseau de communication informatique, à un dispositif contrôleur associé à l'entité contrôleur ; ledit dispositif contrôleur se présentant notamment sous la forme d'un terminal ou d'un serveur distant ;

ledit dispositif terminal permettant d'exécuter les étapes suivantes :

- **étape 1 : acte d'engagement R**

à chaque appel, les moyens de calcul des engagements **R** du dispositif témoin calculent chaque engagement **R** en appliquant le processus spécifié selon la revendication 17,

le dispositif témoin comporte des moyens de transmission, ci-après désignés les moyens de transmission du dispositif témoin, pour transmettre tout ou partie de chaque engagement **R** au dispositif signataire, via les moyens d'interconnexion;

- **étape 2 : acte de défi d**

le dispositif signataire comporte des moyens de calcul, ci-après désignés les moyens de calcul du dispositif signataire, appliquant une fonction d

hachage **h** ayant comme arguments le message **M** et chaque engagement **R** pour calculer un train binaire et extraire de ce train binaire des défis **d** en nombre égal au nombre d'engagements **R**,

- **étape 3 : acte de réponse D**

les moyens de réception des défis **d** reçoivent les défis **d** provenant du dispositif signataire, via les moyens d'interconnexion,

les moyens de calcul des réponses **D** du dispositif témoin calculent les réponses **D** à partir des défis **d** en appliquant le processus spécifié selon la revendication 9,

le dispositif témoin comporte des moyens de transmission, ci-après désignés les moyens de transmission du dispositif témoin, pour transmettre les réponses **D** au dispositif signataire, via les moyens d'interconnexion.

21. Dispositif contrôleur, se présentant notamment sous la forme d'un terminal ou d'un serveur distant, associé à une entité contrôleur, destiné à prouver à un serveur contrôleur,

- l'authenticité d'une entité et/ou
- l'intégrité d'un message **M** associé à cette entité,

au moyen:

- de **m** couples de valeurs privées $Q_1, Q_2, \ldots Q_m$ et publiques $G_1, G_2, \ldots G_m$, **m** étant supérieur ou égal à 1,
- d'un module public **n** constitué par le produit de **f** facteurs premiers $p_1, p_2, \ldots p_f$, **f** étant supérieur ou égal à 2 ;

ledit module, ledit exposant et lesdites valeurs étant liés par des relations du type :

$$G_i \cdot Q_i^v \equiv 1 \ . \bmod n \text{ ou } G_i \equiv Q_i^v \bmod n \ ;$$

v désignant un exposant public ;

Q_i désignant une valeur privée, inconnue du dispositif contrôleur, associée à la valeur publique G_i .

22. Dispositif contrôleur selon la revendication 21 destiné à prouver

l'authenticité d'une entité appelée démonstrateur à une entité appelée contrôleur ;

ledit dispositif contrôleur comportant des moyens de connexion pour le connecter électriquement, électromagnétiquement, optiquement ou de manière acoustique, notamment via un réseau de communication informatique, à un dispositif démonstrateur associé à l'entité démonstrateur;

ledit dispositif contrôleur permettant d'exécuter les étapes suivantes :

- **étape 1 et 2 : acte d'engagement R, acte de défi**

ledit dispositif contrôleur comporte aussi des moyens de réception de tout ou partie des engagements **R** provenant du dispositif démonstrateur, via les moyens de connexion,

le dispositif contrôleur comporte des moyens de productions de défis pour produire, après avoir reçu tout ou partie de chaque engagement **R**, des défis **d** en nombre égal au nombre d'engagements **R**, chaque défi **d** comportant **m** entiers $\mathbf{d_i}$, ci-après appelés défis élémentaires

le dispositif contrôleur comporte aussi des moyens de transmission, ci-après désignés les moyens de transmission du dispositif contrôleur, pour transmettre les défis **d** au démonstrateur, via les moyens de connexion,

- **étapes 3 et 4 : acte de réponse, acte de contrôle**

le dispositif contrôleur comporte aussi

- des moyens de réception des réponses **D** provenant du dispositif démonstrateur, via les moyens de connexion,

- des moyens de calcul, ci-après désignés les moyens de calcul du dispositif contrôleur,

- des moyens de comparaison, ci-après désignés les moyens de comparaison du dispositif contrôleur,

cas où le démonstrateur a transmis une partie de chaque engagement R

dans le cas où les moyens de réception du dispositif contrôleur ont reçus

une partie de chaque engagement **R**, les moyens de calcul du dispositif contrôleur, disposant des **m** valeurs publiques G_1, G_2, ... G_m, calculent à partir de chaque défi **d** et de chaque réponse **D** un engagement reconstruit **R'** satisfaisant à une relation du type :

$$R' \equiv G_1^{d1} . G_2^{d2} . \ldots G_m^{dm} . D^v \bmod n$$

ou à une relation du type,

$$R' \equiv D^v / G_1^{d1} . G_2^{d2} . \ldots G_m^{dm} . \bmod n ,$$

les moyens de comparaison du dispositif contrôleur comparent chaque engagement reconstruit **R'** à tout ou partie de chaque engagement **R** reçus,

cas où le démonstrateur a transmis l'intégralité de chaque engagement R

dans le cas où les moyens de réception du dispositif contrôleur ont reçus l'intégralité de chaque engagement **R**, les moyens de calcul et les moyens de comparaison du dispositif contrôleur, disposant des **m** valeurs publiques G_1, G_2, ... G_m, vérifient que chaque engagement **R** satisfait à une relation du type :

$$R \equiv G_1^{d1} . G_2^{d2} . \ldots G_m^{dm} . D^v \bmod n$$

ou à une relation du type,

$$R \equiv D^v / G_1^{d1} . G_2^{d2} . \ldots G_m^{dm} . \bmod n .$$

23. Dispositif contrôleur selon la revendication 21 destiné à prouver l'intégrité d'un message **M** associé à une entité appelée démonstrateur,

ledit dispositif contrôleur comportant des moyens de connexion pour le connecter électriquement, électromagnétiquement, optiquement ou de manière acoustique, notamment via un réseau de communication informatique, à un dispositif démonstrateur associé à l'entité démonstrateur;

ledit dispositif contrôleur permettant d'exécuter les étapes suivantes :

- **étapes 1 et 2 : acte d'engagement R, acte de défi**

ledit dispositif contrôleur comporte aussi des moyens de réception de

jetons **T** provenant du démonstrateur, via les moyens de connexion,
le dispositif contrôleur comporte aussi des moyens de productions de défis pour produire, après avoir reçu le jeton **T**, des défis **d** en nombre égal au nombre d'engagements **R** , chaque défi **d** comportant **m** entiers, ci-après appelés les défis élémentaires,
le dispositif contrôleur comporte aussi des moyens de transmission, ci-après désignés les moyens de transmission du dispositif contrôleur, pour transmettre les défis **d** au démonstrateur, via les moyens de connexion,

• **étapes 3 et 4 : acte de réponse D, acte de contrôle**

le dispositif contrôleur comporte aussi :

- des moyens de réception des réponses **D** provenant du dispositif démonstrateur, via les moyens de connexion,

le dispositif contrôleur comporte aussi

- des moyens de calcul, ci-après désignés les moyens de calcul du dispositif contrôleur, disposant des **m** valeurs publiques $G_1, G_2, \ldots G_m$, pour d'une part, calculer à partir de chaque défi **d** et de chaque réponse **D** un engagement reconstruit **R'** satisfaisant à une relation du type :

$$R' \equiv G_1^{d1} . G_2^{d2} . \ldots G_m^{dm} . D^v \bmod n$$

ou à une relation du type :

$$R' \equiv D^v / G_1^{d1} . G_2^{d2} . \ldots G_m^{dm} . \bmod n$$

puis d'autre part, calculer en appliquant la fonction de hachage **h** ayant comme arguments le message **M** et tout ou partie de chaque engagement reconstruit **R'**, un jeton **T'**,
le dispositif contrôleur comporte aussi des moyens de comparaison, ci-après désignés les moyens de comparaison du dispositif contrôleur, pour comparer le jeton **T'** au jeton **T** reçu.

24. Dispositif contrôleur selon la revendication 21 destiné à prouver l'authenticité du message **M** en contrôlant, par une entité appelée contrôleur, le message signé;

le message signé, émis par un dispositif signataire associé à une entité signataire disposant d'une fonction de hachage **h (M, R)** ; comprenant:

- le message M,
- les défis **d** et/ou les engagements **R,**
- les réponse **D** ;

ledit dispositif contrôleur comportant des moyens de connexion pour le connecter électriquement, électromagnétiquement, optiquement ou de manière acoustique, notamment via un réseau de communication informatique, à un dispositif signataire associé à l'entité signataire ;

ledit dispositif contrôleur ayant reçu le message signé du dispositif signataire, via les moyens de connexion,

le dispositif contrôleur comporte :

- des moyens de calcul, ci-après désignés les moyens de calcul du dispositif contrôleur,
- des moyens de comparaison, ci-après désignés les moyens de comparaison du dispositif contrôleur,

• cas où le contrôleur dispose des engagements R, des défis d, des réponses D,

dans le cas où le dispositif contrôleur dispose des engagements **R,** des défis **d,** des réponses **D,**

• • les moyens de calcul et de comparaison du dispositif contrôleur vérifient que les engagements **R,** les défis **d** et les réponses **D** satisfont à des relations du type

$$\mathbf{R \equiv G_1^{\,d1} . G_2^{\,d2} . \ldots G_m^{\,dm} . D^v \bmod n}$$

ou à des relations du type :

$$\mathbf{R \equiv D^v / G_1^{\,d1} . G_2^{\,d2} . \ldots G_m^{\,dm} . \bmod n}$$

• • les moyens de calcul et de comparaison du dispositif contrôleur vérifient que le message **M,** les défis **d** et les engagements **R** satisfont à la fonction de hachage

$$d = h(M, R)$$

• **cas où le contrôleur dispose des défis d et des réponses D**

dans le cas où le dispositif contrôleur dispose des défis **d** et des réponses **D**,

•• les moyens de calcul du dispositif contrôleur calculent, à partir de chaque défi **d** et de chaque réponse **D**, des engagements **R'** satisfaisant à des relations du type :

$$R' \equiv G_1^{d1} . G_2^{d2} . \ldots G_m^{dm} . D^v \bmod n$$

ou à des relations du type :

$$R' \equiv D^v / G_1^{d1} . G_2^{d2} . \ldots G_m^{dm} . \bmod n$$

•• les moyens de calcul et de comparaison du dispositif contrôleur vérifie que le message **M** et les défis **d** satisfont à la fonction de hachage

$$d = h(M, R')$$

• **cas où le contrôleur dispose des engagements R et des réponses D**

dans le cas où le dispositif contrôleur dispose des engagements **R** et des réponses **D**,

•• les moyens de calcul du dispositif contrôleur appliquent la fonction de hachage et calculent **d'** tel que

$$d' = h(M, R)$$

•• les moyens de calcul et de comparaison du dispositif contrôleur vérifient que les engagements **R**, les défis **d'** et les réponses **D**, satisfont à des relations du type :

$$R \equiv G_1^{d'1} . G_2^{d'2} . \ldots G_m^{d'm} . D^v \bmod n$$

ou à des relations du type :

$$R \equiv D^v / G_1^{d'1} . G_2^{d'2} . \ldots G_m^{d'm} . \bmod n$$

PCT ORGA TION MONDIALE DE LA PROPRIETE INTELLEC. E
Bureau international

DEMANDE INTERNATIONALE PUBLIEE EN VERTU DU TRAITE DE COOPERATION EN MATIERE DE BREVETS (PCT)

(51) Classification internationale des brevets 7 : H04L

A2

(11) Numéro de publication internationale: **WO 00/46946**

(43) Date de publication internationale: 10 août 2000 (10.08.00)

(21) Numéro de la demande internationale: PCT/FR00/00188

(22) Date de dépôt international: 27 janvier 2000 (27.01.00)

(30) Données relatives à la priorité:

99/01065	27 janvier 1999 (27.01.99)	FR
99/03770	23 mars 1999 (23.03.99)	FR
99/12465	1er octobre 1999 (01.10.99)	FR
99/12467	1er octobre 1999 (01.10.99)	FR
99/12468	1er octobre 1999 (01.10.99)	FR

(71) Déposants *(pour tous les Etats désignés sauf US)*: FRANCE TELECOM [FR/FR]; 6, place d'Alleray, F–75015 Paris (FR). TELEDIFFUSION DE FRANCE [FR/FR]; 10, rue d'Oradour–sur–Glane, F–75732 Paris Cedex 15 (FR). MATH RIZK [BE/BE]; Verte Voie 20, B–1348 Louvain–la–Neuve (BE).

(72) Inventeurs; et

(75) Inventeurs/Déposants *(US seulement)*: GUILLOU, Louis [FR/FR]; 16, rue de l'Ise, F–35230 Bourgbarre (FR). QUISQUATER, Jean–Jacques [BE/BE]; 3, avenue des Canards, B–1640 Rhode Saint Genese (BE).

(74) Mandataire: VIDON, Patrice; Cabinet Patrice Vidon, Immeuble Germanium, 80, avenue des Buttes de Coësmes, F–35700 Rennes (FR).

(81) Etats désignés: AE, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CR, CU, CZ, DE, DK, DM, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZW, brevet ARIPO (GH, GM, KE, LS, MW, SD, SL, SZ, TZ, UG, ZW), brevet eurasien (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), brevet européen (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), brevet OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

Publiée

Sans rapport de recherche internationale, sera republiée dès réception de ce rapport.

(54) Title: METHOD, SYSTEM, DEVICE FOR PROVING THE AUTHENTICITY OF AN ENTITY AND/OR THE INTEGRITY AND/OR THE AUTHENTICITY OF A MESSAGE

(54) Titre: PROCEDE, SYSTEME, DISPOSITIF DESTINES A PROUVER L'AUTHENTICITE D'UNE ENTITE ET/OU L'INTEGRITE ET/OU L'AUTHENTICITE D'UN MESSAGE

(57) Abstract

The proof is provided by the following parameters: m pairs of private values Q_i and public values P_i, m>1; a public module n formed by the product of f first factors p_i, f>2; a public exponent v, bound by the relationship of the type: $G_i.Q_i^v \equiv \text{mod } n$ or $G_i \equiv Q_i^v \text{ mod } n$.

(57) Abrégé

La preuve est établie au moyen des paramètres suivants: m couples de valeurs privées Q_i et publiques P_i, m>1, un module public n constitué par le produit de f facteurs premiers p_i, f>2, un exposant public v, liés par des relations du type: $G_i.Q_i^v \equiv 1 \text{ mod } n$ ou $G_i \equiv Q_i^v \text{ mod } n$.

UNIQUEMENT A TITRE D'INFORMATION

Codes utilisés pour identifier les Etats parties au PCT, sur les pages de couverture des brochures publiant des demandes internationales en vertu du PCT.

AL	Albanie	**ES**	Espagne	**LS**	Lesotho	**SI**	Slovénie
AM	Arménie	**FI**	Finlande	**LT**	Lituanie	**SK**	Slovaquie
AT	Autriche	**FR**	France	**LU**	Luxembourg	**SN**	Sénégal
AU	Australie	**GA**	Gabon	**LV**	Lettonie	**SZ**	Swaziland
AZ	Azerbaïdjan	**GB**	Royaume-Uni	**MC**	Monaco	**TD**	Tchad
BA	Bosnie-Herzégovine	**GE**	Géorgie	**MD**	République de Moldova	**TG**	Togo
BB	Barbade	**GH**	Ghana	**MG**	Madagascar	**TJ**	Tadjikistan
BE	Belgique	**GN**	Guinée	**MK**	Ex-République yougoslave de Macédoine	**TM**	Turkménistan
BF	Burkina Faso	**GR**	Grèce			**TR**	Turquie
BG	Bulgarie	**HU**	Hongrie	**ML**	Mali	**TT**	Trinité-et-Tobago
BJ	Bénin	**IE**	Irlande	**MN**	Mongolie	**UA**	Ukraine
BR	Brésil	**IL**	Israël	**MR**	Mauritanie	**UG**	Ouganda
BY	Bélarus	**IS**	Islande	**MW**	Malawi	**US**	Etats-Unis d'Amérique
CA	Canada	**IT**	Italie	**MX**	Mexique	**UZ**	Ouzbékistan
CF	République centrafricaine	**JP**	Japon	**NE**	Niger	**VN**	Viet Nam
CG	Congo	**KE**	Kenya	**NL**	Pays-Bas	**YU**	Yougoslavie
CH	Suisse	**KG**	Kirghizistan	**NO**	Norvège	**ZW**	Zimbabwe
CI	Côte d'Ivoire	**KP**	République populaire démocratique de Corée	**NZ**	Nouvelle-Zélande		
CM	Cameroun			**PL**	Pologne		
CN	Chine	**KR**	République de Corée	**PT**	Portugal		
CU	Cuba	**KZ**	Kazakstan	**RO**	Roumanie		
CZ	République tchèque	**LC**	Sainte-Lucie	**RU**	Fédération de Russie		
DE	Allemagne	**LI**	Liechtenstein	**SD**	Soudan		
DK	Danemark	**LK**	Sri Lanka	**SE**	Suède		
EE	Estonie	**LR**	Libéria	**SG**	Singapour		

Procédé, système, dispositif destinés à prouver l'authenticité d'une entité et/ou l'intégrité et/ou l'authenticité d'un message.

La présente invention concerne les procédés, les systèmes ainsi que les dispositifs destinés à prouver l'authenticité d'une entité et/ou l'intégrité et/ou l'authenticité d'un message.

Le brevet EP 0 311 470 B1 dont les inventeurs sont Louis Guillou et Jean-Jacques Quisquater décrit un tel procédé. On y fera ci-après référence en le désignant par les termes : "brevet GQ" ou "procédé GQ". Par la suite on désignera parfois par "GQ2", "invention GQ2" ou "technologie GQ2" la présente invention.

Selon le procédé GQ, une entité appelée " autorité de confiance " attribue une identité à chaque entité appelée " témoin" et en calcule la signature RSA; durant un processus de personnalisation, l'autorité de confiance donne identité et signature au témoin. Par la suite, le témoin proclame : "*Voici mon identité ; j'en connais la signature RSA.*" Le témoin prouve sans la révéler qu'il connaît la signature RSA de son identité. Grâce à la clé publique de vérification RSA distribuée par l'autorité de confiance, une entité appelée "contrôleur" vérifie sans en prendre connaissance que la signature RSA correspond à l'identité proclamée. Les mécanismes utilisant le procédé GQ se déroulent "sans transfert de connaissance". Selon le procédé GQ le témoin ne connaît pas la clé privée RSA avec laquelle l'autorité de confiance signe un grand nombre d'identités.

Le procédé GQ met en œuvre des calculs modulo des nombres de 512 bits ou davantage. Ces calculs concernent des nombres ayant sensiblement la même taille élevés à des puissances de l'ordre de $2^{16} + 1$. Or les infrastructures microélectroniques existantes, notamment dans le domaine des cartes bancaires, font usage de microprocesseurs auto-programmables monolithiques dépourvus de coprocesseurs arithmétiques. La charge de travail liée aux multiples opérations arithmétiques impliquées par des

procédés tels que le procédé GQ, entraîne des temps de calcul qui dans certains cas s'avèrent pénalisant pour les consommateurs utilisant des cartes bancaires pour acquitter leurs achats. Il est rappelé ici, qu'en cherchant à accroître la sécurité des cartes de paiement, les autorités bancaires posent un problème particulièrement délicat à résoudre. En effet, il faut traiter deux questions apparemment contradictoires : augmenter la sécurité en utilisant des clés de plus en plus longues et distinctes pour chaque carte tout en évitant que la charge de travail n'entraîne des temps de calcul prohibitifs pour les utilisateurs. Ce problème prend un relief particulier dans la mesure où, en outre, il convient de tenir compte de l'infrastructure en place et des composants microprocesseurs existants.

La technologie GQ précédemment décrite fait appel à la technologie RSA. Mais si la technologie RSA dépend bel et bien de la factorisation du module n, cette dépendance n'est pas une équivalence, loin s'en faut, comme le démontrent les attaques dites "multiplicatives" contre les diverses normes de signature numérique mettant en oeuvre la technologie RSA.

L'objectif de la technologie GQ2 est double : d'une part, améliorer les performances par rapport à la technologie RSA ; d'autre part, éviter les problèmes inhérents à la technologie RSA. La connaissance de la clé privée GQ2 est équivalente à la connaissance de la factorisation du module n. Toute attaque au niveau des triplets GQ2 se ramène à la factorisation du module n : il y a cette fois équivalence. Avec la technologie GQ2, la charge de travail est réduite, tant pour l'entité qui signe ou qui s'authentifie que pour celle qui contrôle. Grâce à un meilleur usage du problème de la factorisation, tant en sécurité qu'en performance, la technologie GQ2 évite les inconvénients présentés par la technologie RSA.

Procédé

Méthode des restes chinois appliquée à la famille GQ

Plus particulièrement, l'invention concerne un procédé destiné à prouver à

une entité contrôleur,

- l'authenticité d'une entité et/ou
- l'intégrité d'un message **M** associé à cette entité.

Cette preuve est établie au moyen de tout ou partie des paramètres suivants ou dérivés de ceux-ci:

- **m** couples de valeurs privées $Q_1, Q_2, \ldots Q_m$ et publiques $G_1, G_2, \ldots G_m$ (**m** étant supérieur ou égal à 1),
- un module public **n** constitué par le produit de **f** facteurs premiers $p_1, p_2, \ldots p_f$ (**f** étant supérieur ou égal à 2),
- un exposant public **v** .

Ledit module, ledit exposant et lesdites valeurs sont liés par des relations du type :

$$G_i \cdot Q_i^v \equiv 1 \ . \mathbf{mod}\ n \text{ ou } G_i \equiv Q_i^v \ \mathbf{mod}\ n \ ;$$

Ledit procédé met en œuvre selon les étapes ci-après définies une entité appelée témoin disposant des **f** facteurs premiers p_i et/ou des paramètres des restes chinois des facteurs premiers et/ou du module public **n** et/ou des **m** valeurs privées Q_i et/ou des **f.m** composantes $Q_{i,j}$ ($Q_{i,j} \equiv Q_i \ \mathbf{mod}\ p_j$) des valeurs privées Q_i et de l'exposant public **v** .

Le témoin calcule des engagements **R** dans l'anneau des entiers modulo **n**. Chaque engagement est calculé en effectuant des opérations du type

$$R_i \equiv r_i^v \ \mathbf{mod}\ p_i$$

où r_i est un aléa associé au nombre premier p_i tel que $0 < r_i < p_i$, chaque r_i appartenant à une collection d'aléas $\{r_1 , r_2 , \ldots r_t\}$, puis en appliquant la méthode des restes chinois,

Ainsi, le nombre d'opérations arithmétiques modulo p_i à effectuer pour calculer chacun des engagements R_i pour chacun des p_i est réduit par rapport à ce qu'il serait si les opérations étaient effectuées modulo n.

Le témoin reçoit un ou plusieurs défis **d**. Chaque défi **d** comportant **m** entiers d_i ci-après appelés défis élémentaires. Le témoin calcule à partir de

chaque défi **d** une réponse **D**, en effectuant des opérations du type :

$$D_i \equiv r_i \cdot Q_{i,1}^{d1} \cdot Q_{i,2}^{d2} \cdot \ldots Q_{i,m}^{dm} \bmod p_i$$

puis en appliquant la méthode des restes chinois.

Ainsi, le nombre d'opérations arithmétiques modulo p_i à effectuer pour calculer chacune des réponses D_i pour chacun des p_i est réduit par rapport à ce qu'il serait si les opérations étaient effectuées modulo n.

Le procédé est tel qu'il y a autant de réponses **D** que de défis **d** que d'engagements **R**, chaque groupe de nombres **R, d, D** constituant un triplet noté **{R, d, D}.**

Cas de la preuve de l'authenticité d'une entité

Dans une première variante de réalisation le procédé selon l'invention est destiné à prouver l'authenticité d'une entité appelée démonstrateur à une entité appelée contrôleur. Ladite entité démonstrateur comprend le témoin. Lesdites entités démonstrateur et contrôleur exécutent les étapes suivantes:

- **étape 1 : acte d'engagement R**

A chaque appel, le témoin calcule chaque engagement **R** en appliquant le processus spécifié ci-dessus. Le démonstrateur transmet au contrôleur tout ou partie de chaque engagement **R.**

- **étape 2 : acte de défi d**

Le contrôleur, après avoir reçu tout ou partie de chaque engagement **R,** produit des défis **d** en nombre égal au nombre d'engagements **R** et transmet les défis **d** au démonstrateur.

- **étape 3 : acte de réponse D**

Le témoin calcule des réponses **D** à partir des défis **d** en appliquant le processus spécifié ci-dessus.

- **étape 4 : acte de contrôle**

Le démonstrateur transmet chaque réponse **D** au contrôleur.

Premier cas : le démonstrateur a transmis une partie de chaque engagement R

Dans le cas où le démonstrateur a transmis une partie de chaque engagement **R**, le contrôleur, disposant des **m** valeurs publiques G_1, G_2, ... G_m, calcule à partir de chaque défi **d** et de chaque réponse **D** un engagement reconstruit **R'** satisfaisant à une relation du type :

$$R' \equiv G_1^{d1} . G_2^{d2} . \ldots G_m^{dm} . D^v \bmod n$$

ou à une relation du type,

$$R' \equiv D^v / G_1^{d1} . G_2^{d2} . \ldots G_m^{dm} . \bmod n .$$

Le contrôleur vérifie que chaque engagement reconstruit **R'** reproduit tout ou partie de chaque engagement **R** qui lui a été transmis.

Deuxième cas : le démonstrateur a transmis l'intégralité de chaque engagement R

Dans le cas où le démonstrateur a transmis l'intégralité de chaque engagement **R**, le contrôleur, disposant des **m** valeurs publiques G_1, G_2, ... G_m, vérifie que chaque engagement **R** satisfait à une relation du type :

$$R \equiv G_1^{d1} . G_2^{d2} . \ldots G_m^{dm} . D^v \bmod n$$

ou à une relation du type,

$$R \equiv D^v / G_1^{d1} . G_2^{d2} . \ldots G_m^{dm} . \bmod n .$$

Cas de la preuve de l'intégrité d'un message

dans une deuxième variante de réalisation susceptible d'être combinée avec la première, le procédé selon l'invention est destiné à prouver à une entité appelée contrôleur l'intégrité d'un message **M** associé à une entité appelée démonstrateur. Ladite entité démonstrateur comprend le témoin.

Lesdites entités démonstrateur et contrôleur exécutent les étapes suivantes:

- **étape 1 : acte d'engagement R**

A chaque appel, le témoin calcule chaque engagement **R** en appliquant le processus spécifié ci-dessus.

- **étape 2 : acte de défi d**

Le démonstrateur applique une fonction de hachage **h** ayant comme arguments le message **M** et tout ou partie de chaque engagement **R** pour

calculer au moins un jeton T. Le démonstrateur transmet le jeton **T** au contrôleur. Le contrôleur, après avoir reçu un jeton **T**, produit des défis **d** en nombre égal au nombre d'engagements **R** et transmet les défis **d** a u démonstrateur.

• **étape 3 : acte de réponse D**

Le témoin calcule des réponses **D** à partir des défis **d** en appliquant le processus spécifié ci-dessus.

• **étape 4 : acte de contrôle**

Le démonstrateur transmet chaque réponse **D** au contrôleur Le contrôleur, disposant des m valeurs publiques $G_1, G_2, \ldots G_m$, calcule à partir de chaque défi **d** et de chaque réponse **D** un engagement reconstruit **R'** satisfaisant à une relation du type :

$$R' \equiv G_1^{d1} . G_2^{d2} . \ldots G_m^{dm} . D^v \bmod n$$

ou à une relation du type :

$$R' \equiv D^v / G_1^{d1} . G_2^{d2} . \ldots G_m^{dm} . \bmod n.$$

Puis, le contrôleur applique la fonction de hachage **h** ayant comme arguments le message **M** et tout ou partie de chaque engagement reconstruit **R'** pour reconstruire le jeton **T'**. Puis, le contrôleur vérifie que le jeton **T'** est identique au jeton **T** transmis.

Signature numérique d'un message et preuve de son authenticité

Opération de signature

Dans une troisième variante de réalisation susceptible d'être prise en combinaison avec l'une et/ou l'autre des autres variantes de réalisation, le procédé selon l'invention est destiné à produire la signature numérique d'un message **M** par une entité appelée entité signataire. Ladite entité signataire comprend le témoin.

Ladite entité signataire exécute une opération de signature en vue d'obtenir un message signé comprenant :

- le message **M**,

- les défis **d** et/ou les engagements **R**,
- les réponses **D**.

Ladite entité signataire exécute l'opération de signature en mettant en oeuvre les étapes suivantes :

• **étape 1 : acte d'engagement R**

A chaque appel, le témoin calcule chaque engagement **R** en appliquant le processus spécifié ci-dessus.

• **étape 2 : acte de défi d**

Le signataire applique une fonction de hachage **h** ayant comme arguments le message **M** et chaque engagement **R** pour obtenir un train binaire. Le signataire extrait de ce train binaire des défis **d** en nombre égal au nombre d'engagements **R.**

• **étape 3 : acte de réponse D**

Le témoin calcule des réponses **D** à partir des défis **d** en appliquant le processus spécifié ci-dessus.

Opération de contrôle

Pour l'authenticité du message **M**, une entité, appelée contrôleur, contrôle le message signé. Ladite entité contrôleur disposant du message signé exécute une opération de contrôle en procédant comme ci-après décrit.

• **cas où le contrôleur dispose des engagements R, des défis d, des réponses D,**

Dans le cas où le contrôleur dispose des engagements **R,** des défis **d,** des réponses **D,** le contrôleur vérifie que les engagements **R**, les défis **d** et les réponses **D** satisfont à des relations du type

$$R \equiv G_1^{d1} . G_2^{d2} . \ldots G_m^{dm} . D^v \bmod n$$

ou à des relations du type :

$$R \equiv D^v / G_1^{d1} . G_2^{d2} . \ldots G_m^{dm} . \bmod n$$

Puis, le contrôleur vérifie que le message **M,** les défis **d** et les engagements **R** satisfont à la fonction de hachage

$$d = h(M, R)$$

• cas où le contrôleur dispose des défis d et des réponses D

Dans le cas où le contrôleur dispose des défis **d** et des réponses **D**, le contrôleur reconstruit, à partir de chaque défi **d** et de chaque réponse **D**, des engagements **R'** satisfaisant à des relations du type :

$$R' \equiv G_1^{d1} . G_2^{d2} . \ldots G_m^{dm} . D^v \bmod n$$

ou à des relations du type :

$$R' \equiv D^v / G_1^{d1} . G_2^{d2} . \ldots G_m^{dm} . \bmod n$$

Puis, le contrôleur vérifie que le message **M** et les défis **d** satisfont à la fonction de hachage

$$d = h(M, R')$$

• cas où le contrôleur dispose des engagements R et des réponses D

Dans le cas où le contrôleur dispose des engagements **R** et des réponses **D**, le contrôleur applique la fonction de hachage et reconstruit **d'**

$$d' = h(M, R)$$

Puis, le contrôleur vérifie que les engagements **R**, les défis **d'** et les réponses **D**, satisfont à des relations du type :

$$R \equiv G_1^{d'1} . G_2^{d'2} . \ldots G_m^{d'm} . D^v \bmod n$$

ou à des relations du type :

$$R \equiv D^v / G_1^{d'1} . G_2^{d'2} . \ldots G_m^{d'm} . \bmod n.$$

Cas où on choisit la valeur privée Q en premier et où on déduit la valeur publique G de la valeur privée Q

Dans certains, notamment afin de faciliter la production des couples de valeurs privées **Q** et publiques **G**, on choisit la valeur privée **Q** en premier et on déduit la valeur publique **G** de la valeur privée **Q**. Plus particulièrement dans ce cas, le procédé selon l'invention est tel que les composantes $Q_{i,1}$, $Q_{i,2}$, ... $Q_{i,f}$ des valeurs privées Q_i, sont des nombres tirés au hasard à raison d'une composante $Q_{i\,j}$ ($Q_{i,j} \equiv Q_i \bmod p_j$) pour chacun desdits facteurs premiers p_j. Lesdites valeurs privées Q_i peuvent

être calculées à partir desdites composantes $Q_{i,1}$, $Q_{i,2}$ ... $Q_{i,f}$ par la méthode des restes chinois. Lesdites valeurs publiques G_i, sont calculées en effectuant des opérations du type

$$G_{i,j} \equiv Q_{i,j}^{\ v} \bmod p_j$$

puis, en appliquant la méthode des restes chinois pour établir G_i tel que

$$G_i \cdot Q_i^v \equiv 1 \cdot \bmod n \text{ ou } G_i \equiv Q_i^{-v} \bmod n ;$$

Ainsi, le nombre d'opérations arithmétiques modulo p_i à effectuer pour calculer chacun des $G_{i,j}$ pour chacun des p_j est réduit par rapport à ce qu'il serait si les opérations étaient effectuées modulo **n**.

Avantageusement dans ce cas, le procédé selon l'invention est tel que l'exposant public de vérification **v** est un nombre premier. On démontre que la sécurité est équivalente à la connaissance de la valeur privée Q_i .

Cas où on choisit la valeur publique G en premier et où on déduit la valeur privée Q de la valeur publique G.

De préférence dans ce cas, ledit exposant **v** est tel que

$$v = 2^k$$

où **k** est un paramètre de sécurité plus grand que 1 .

Ladite valeur publique G_i est le carré g_i^2 d'un nombre de base g_i inférieur aux **f** facteurs premiers $p_1, p_2, \ldots p_f$. Le nombre de base g_i est tel que les deux équations :

$$x^2 \equiv g_i \bmod n \qquad \text{et} \qquad x^2 \equiv -g_i \bmod n$$

n'ont pas de solution en x dans l'anneau des entiers modulo **n** et tel que l'équation :

$$x^v \equiv g_i^2 \bmod n$$

a des solutions en x dans l'anneau des entiers modulo **n**.

Système

La présente invention concerne également un système destiné à prouver à un serveur contrôleur,

- l'authenticité d'une entité et/ou

- l'intégrité d'un message **M** associé à cette entité.

Cette preuve est établie au moyen de tout ou partie des paramètres suivants ou dérivés de ceux-ci:

- **m** couples de valeurs privées $Q_1, Q_2, \ldots Q_m$ et publiques $G_1, G_2, \ldots G_m$ (**m** étant supérieur ou égal à 1),

- un module public **n** constitué par le produit de **f** facteurs premiers $p_1, p_2, \ldots p_f$ (**f** étant supérieur ou égal à 2),

- un exposant public **v** .

Ledit module, ledit exposant et lesdites valeurs étant liés par des relations du type :

$$G_i \cdot Q_i^v \equiv 1 \ . \mathbf{mod}\ n \text{ ou } G_i \equiv Q_i^v \mathbf{mod}\ n \ .$$

Ledit système comprend un dispositif témoin, notamment contenu dans un objet nomade se présentant par exemple sous la forme d'une carte bancaire à microprocesseur. Le dispositif témoin comporte une zone mémoire contenant les **f** facteurs premiers p_i et/ou des paramètres des restes chinois des facteurs premiers et/ou du module public **n** et/ou des **m** valeurs privées Q_i et/ou des **f.m** composantes $Q_{i,j}$ ($Q_{i,j} \equiv Q_i \mathbf{mod}\ p_j$) des valeurs privées Q_i et de l'exposant public **v**. Le dispositif témoin comporte aussi :

- des moyens de production d'aléas, ci-après désignés les moyens de production d'aléas du dispositif témoin,

- des moyens de calcul, ci-après désignés les moyens de calcul des engagements **R** du dispositif témoin, pour calculer des engagements **R** dans l'anneau des entiers modulo **n**. Chaque engagement est calculé en effectuant des opérations du type

$$R_i \equiv r_i^v \mathbf{mod}\ p_i$$

où r_i est un aléa associé au nombre premier p_i tel que $0 < r_i < p_i$, chaque r_i appartenant à une collection d'aléas $\{r_1 , r_2 , \ldots r_f\}$ produits par les moyens de production d'aléas, puis en appliquant la méthode des restes chinois.

Ainsi, le nombre d'opérations arithmétiques modulo p_i à effectuer pour

calculer chacun des engagements $\mathbf{R_i}$ pour chacun des $\mathbf{p_i}$ est réduit par rapport à ce qu'il serait si les opérations étaient effectuées modulo n.

Le dispositif témoin comporte aussi :

- des moyens de réception, ci-après désignés les moyens de réception des défis **d** du dispositif témoin, pour recevoir un ou plusieurs défis **d** ; chaque défi **d** comportant **m** entiers $\mathbf{d_i}$ ci-après appelés défis élémentaires ;

- des moyens de calcul, ci-après désignés les moyens de calcul des réponses **D** du dispositif témoin, pour calculer à partir de chaque défi **d** une réponse **D** en effectuant des opérations du type :

$$\mathbf{D_i \equiv r_i \cdot Q_{i,1}^{\,d1} \cdot Q_{i,2}^{\,d2} \cdot \ldots \; Q_{i,m}^{\,dm} \bmod p_i}$$

puis, en appliquant la méthode des restes chinois.

Ainsi, le nombre d'opérations arithmétiques modulo p_i à effectuer pour calculer chacune des réponses D_i pour chacun des p_i est réduit par rapport à ce qu'il serait si les opérations étaient effectuées modulo n.

Ledit dispositif témoin comporte aussi des moyens de transmission pour transmettre un ou plusieurs engagements **R** et une ou plusieurs réponses **D.** Il y a autant de réponses **D** que de défis **d** que d'engagements **R.** Chaque groupe de nombres **R, d, D** constituant un triplet noté **{R, d, D}.**

Cas de la preuve de l'authenticité d'une entité

Dans une première variante de réalisation le système selon l'invention est destiné à prouver l'authenticité d'une entité appelée démonstrateur à une entité appelée contrôleur.

Ledit système est tel qu'il comporte un dispositif démonstrateur associé à l'entité démonstrateur. Ledit dispositif démonstrateur est interconnecté au dispositif témoin par des moyens d'interconnexion. Il peut se présenter notamment sous la forme de microcircuits logiques dans un objet nomade par exemple sous la forme d'un microprocesseur dans une carte bancaire à microprocesseur.

Ledit système comporte aussi un dispositif contrôleur associé à l'entité

contrôleur. Ledit dispositif contrôleur se présente notamment sous la forme d'un terminal ou d'un serveur distant. Ledit dispositif contrôleur comporte des moyens de connexion pour le connecter électriquement, électromagnétiquement, optiquement ou de manière acoustique, notamment via un réseau de communication informatique, au dispositif démonstrateur.

Ledit système permet d'exécuter les étapes suivantes :

- **étape 1 : acte d'engagement R**

A chaque appel, les moyens de calcul des engagements **R** du dispositif témoin calculent chaque engagement **R** en appliquant le processus spécifié ci-dessus. Le dispositif témoin comporte des moyens de transmission, ci-après désignés les moyens de transmission du dispositif témoin, pour transmettre tout ou partie de chaque engagement **R** au dispositif démonstrateur, via les moyens d'interconnexion. Le dispositif démonstrateur comporte aussi des moyens de transmission, ci-après désigné les moyens de transmission du dispositif démonstrateur, pour transmettre tout ou partie de chaque engagement **R** au dispositif contrôleur, via les moyens de connexion.

- **étape 2 : acte de défi d**

Le dispositif contrôleur comporte des moyens de productions de défis pour produire, après avoir reçu tout ou partie de chaque engagement **R**, des défis **d** en nombre égal au nombre d'engagements **R.** Le dispositif contrôleur comporte aussi des moyens de transmission, ci-après désignés les moyens de transmission du contrôleur, pour transmettre les défis **d** au démonstrateur, via les moyens de connexion.

- **étape 3 : acte de réponse D**

Les moyens de réception des défis **d** du dispositif témoin, reçoivent chaque défi **d** provenant du dispositif démonstrateur, via les moyens d'interconnexion. Les moyens de calcul des réponses **D** du dispositif témoin calculent les réponses **D** à partir des défis **d** en appliquant le processus

spécifié ci-dessus.

• **étape 4 : acte de contrôle**

Les moyens de transmission du démonstrateur transmettent chaque réponse **D** au contrôleur. Le dispositif contrôleur comporte aussi

- des moyens de calcul, ci-après désignés les moyens de calcul du dispositif contrôleur,

- des moyens de comparaison, ci-après désignés les moyens de comparaison du dispositif contrôleur.

Premier cas : le démonstrateur a transmis une partie de chaque engagement R

Dans le cas où les moyens de transmission du démonstrateur ont transmis une partie de chaque engagement **R**, les moyens de calcul du dispositif contrôleur, disposant des **m** valeurs publiques G_1, G_2, ... G_m, calculent à partir de chaque défi **d** et de chaque réponse **D** un engagement reconstruit **R'** satisfaisant à une relation du type :

$$R' \equiv G_1^{d1} . G_2^{d2} . \ldots G_m^{dm} . D^v \bmod n$$

ou à une relation du type,

$$R' \equiv D^v / G_1^{d1} . G_2^{d2} . \ldots G_m^{dm} . \bmod n .$$

Les moyens de comparaison du dispositif contrôleur comparent chaque engagement reconstruit **R'** à tout ou partie de chaque engagement **R** reçu.

cas où le démonstrateur a transmis l'intégralité de chaque engagement R

Dans le cas où les moyens de transmission du démonstrateur ont transmis l'intégralité de chaque engagement **R**, les moyens de calcul et les moyens de comparaison du dispositif contrôleur, disposant des **m** valeurs publiques G_1, G_2, ... G_m, vérifient que chaque engagement **R** satisfait à une relation du type :

$$R \equiv G_1^{d1} . G_2^{d2} . \ldots G_m^{dm} . D^v \bmod n$$

ou à une relation du type,

$$R \equiv D^v / G_1^{d1} . G_2^{d2} . \ldots G_m^{dm} . \mathbf{mod\ n} .$$

Cas de la preuve de l'intégrité d'un message

Dans une deuxième variante de réalisation susceptible d'être combinée avec la première, le système selon l'invention est destiné à prouver à une entité appelée contrôleur l'intégrité d'un message **M** associé à une entité appelée démonstrateur. Ledit système est tel qu'il comporte un dispositif démonstrateur associé à l'entité démonstrateur. Ledit dispositif démonstrateur est interconnecté au dispositif témoin par des moyens d'interconnexion. Il peut se présenter notamment sous la forme de microcircuits logiques dans un objet nomade par exemple sous la forme d'un microprocesseur dans une carte bancaire à microprocesseur. Ledit système comporte aussi un dispositif contrôleur associé à l'entité contrôleur. Ledit dispositif contrôleur se présente notamment sous la forme d'un terminal ou d'un serveur distant. Ledit dispositif contrôleur comporte des moyens de connexion pour le connecter électriquement, électromagnétiquement, optiquement ou de manière acoustique, notamment via un réseau de communication informatique, au dispositif démonstrateur.
Ledit système exécute les étapes suivantes :

- **étape 1 : acte d'engagement R**

A chaque appel, les moyens de calcul des engagements **R** du dispositif témoin calculent chaque engagement **R** en appliquant le processus spécifié ci-dessus. Le dispositif témoin comporte des moyens de transmission, ci-après désignés les moyens de transmission du dispositif témoin, pour transmettre tout ou partie de chaque engagement **R** au dispositif démonstrateur, via les moyens d'interconnexion.

- **étape 2 : acte de défi d**

Le dispositif démonstrateur comporte des moyens de calcul, ci-après désignés les moyens de calcul du dispositif démonstrateur, appliquant une fonction de hachage **h** ayant comme arguments le message **M** et tout ou

partie de chaque engagement **R** pour calculer au moins un jeton **T**. Le dispositif démonstrateur comporte aussi des moyens de transmission, ci-après désignés les moyens de transmission du démonstrateur, pour transmettre chaque jeton **T** , via les moyens de connexion, au dispositif au contrôleur. Le dispositif contrôleur comporte aussi des moyens de productions de défis pour produire, après avoir reçu le jeton **T**, des défis **d** en nombre égal au nombre d'engagements **R**, Le dispositif contrôleur comporte aussi des moyens de transmission, ci-après désignés les moyens de transmission du dispositif contrôleur, pour transmettre les défis **d** au démonstrateur, via les moyens de connexion.

- **étape 3 : acte de réponse D**

Les moyens de réception des défis **d** du dispositif témoin, reçoivent chaque défi **d** provenant du dispositif démonstrateur, via les moyens d'interconnexion. Les moyens de calcul des réponses **D** du dispositif témoin calculent les réponses **D** à partir des défis **d** en appliquant le processus spécifié ci-dessus.

- **étape 4 : acte de contrôle**

Les moyens de transmission du démonstrateur transmettent chaque réponse **D** au contrôleur. Le dispositif contrôleur comporte aussi des moyens de calcul, ci-après désignés les moyens de calcul du dispositif contrôleur, disposant des **m** valeurs publiques $G_1, G_2, \ldots G_m$, pour d'une part, calculer à partir de chaque défi **d** et de chaque réponse **D** un engagement reconstruit **R'** satisfaisant à une relation du type :

$$R' \equiv G_1^{d1} . G_2^{d2} . \ldots . G_m^{dm} . D^v \bmod n$$

ou à une relation du type :

$$R' \equiv D^v / G_1^{d1} . G_2^{d2} . \ldots . G_m^{dm} . \bmod n$$

puis d'autre part, calculer en appliquant la fonction de hachage **h** ayant comme arguments le message **M** et tout ou partie de chaque engagement reconstruit **R'**, un jeton **T'**.

Le dispositif contrôleur comporte aussi des moyens de comparaison, ci-après désignés les moyens de comparaison du dispositif contrôleur, pour comparer le jeton **T'** au jeton **T** reçu.

Signature numérique d'un message et preuve de son authenticité

Opération de signature

Dans une troisième variante de réalisation, susceptible d'être combinée à l'une et/ou à l'autre des deux autres, le système selon l'invention est destiné à produire la signature numérique d'un message **M**, ci après désigné le message signé, par une entité appelée entité signataire.

Le message signé comprend :

- le message **M**,
- les défis **d** et/ou les engagements **R**,
- les réponses **D** .

Ledit système est tel qu'il comporte un dispositif signataire associé à l'entité signataire. Ledit dispositif signataire est interconnecté au dispositif témoin par des moyens d'interconnexion et peut se présenter notamment sous la forme de microcircuits logiques dans un objet nomade par exemple sous la forme d'un microprocesseur dans une carte bancaire à microprocesseur.

Ledit système permet d'exécuter les étapes suivantes :

- **étape 1 : acte d'engagement R**

A chaque appel, les moyens de calcul des engagements **R** du dispositif témoin calculent chaque engagement **R** en appliquant le processus spécifié ci-dessus.

Le dispositif témoin comporte des moyens de transmission, ci-après désignés les moyens de transmission du dispositif témoin, pour transmettre tout ou partie de chaque engagement **R** au dispositif signataire, via les moyens d'interconnexion.

- **étape 2 : acte de défi d**

Le dispositif signataire comporte des moyens de calcul, ci-après désignés les moyens de calcul du dispositif signataire, appliquant une fonction d hachage **h** ayant comme arguments le message **M** et tout ou partie de chaque engagement **R** pour calculer un train binaire et extraire de ce train binaire des défis **d** en nombre égal au nombre d'engagements **R.**

- **étape 3 : acte de réponse D**

Les moyens de réception des défis **d** du dispositif témoin, reçoivent chaque défi **d** provenant du dispositif signataire, via les moyens d'interconnexion. Les moyens de calcul des réponses **D** du dispositif témoin calculent les réponses **D** à partir des défis **d** en appliquant le processus spécifié ci-dessus. Le dispositif témoin comporte des moyens de transmission, ci-après désignés les moyens de transmission du dispositif témoin, pour transmettre les réponses **D** au dispositif signataire, via les moyens d'interconnexion.

Opération de contrôle

Pour prouver l'authenticité du message **M**, par une entité appelée contrôleur, contrôle le message signé.

Le système comporte un dispositif contrôleur associé à l'entité contrôleur. Ledit dispositif contrôleur se présente notamment sous la forme d'un terminal ou d'un serveur distant. Ledit dispositif contrôleur comporte des moyens de connexion pour le connecter électriquement, électromagnétiquement, optiquement ou de manière acoustique, notamment via un réseau de communication informatique, au dispositif démonstrateur. Ledit dispositif signataire associé à l'entité signataire comporte des moyens de transmission, ci-après désignés les moyens de transmission du dispositif signataire, pour transmettre au dispositif contrôleur, le message signé, via les moyens de connexion. Ainsi, le dispositif contrôleur dispose d'un message signé comprenant:

- le message **M**,
- les défis **d** et/ou les engagements **R**,

- les réponse **D.**

Le dispositif contrôleur comporte :

- des moyens de calcul, ci-après désignés les moyens de calcul du dispositif contrôleur,

- des moyens de comparaison, ci-après désignés les moyens de comparaison du dispositif contrôleur.

• cas où le contrôleur dispose des engagements R, des défis d, des réponses D,

Dans le cas où le dispositif contrôleur dispose des engagements **R,** des défis **d,** des réponses **D,** les moyens de calcul et de comparaison du dispositif contrôleur vérifient que les engagements **R**, les défis **d** et les réponses **D** satisfont à des relations du type

$$R \equiv G_1^{d1} . G_2^{d2} . \ldots G_m^{dm} . D^v \bmod n$$

ou à des relations du type :

$$R \equiv D^v / G_1^{d1} . G_2^{d2} . \ldots G_m^{dm} . \bmod n$$

Puis, les moyens de calcul et de comparaison du dispositif contrôleur vérifient que le message **M,** les défis **d** et les engagements **R** satisfont à la fonction de hachage

$$d = h(M, R)$$

• cas où le contrôleur dispose des défis d et des réponses D

Dans le cas où le dispositif contrôleur dispose des défis **d** et des réponses **D,** les moyens de calcul du dispositif contrôleur calculent, à partir de chaque défi **d** et de chaque réponse **D**, des engagements **R'** satisfaisant à des relations du type :

$$R' \equiv G_1^{d1} . G_2^{d2} . \ldots G_m^{dm} . D^v \bmod n$$

ou à des relations du type :

$$R' \equiv D^v / G_1^{d1} . G_2^{d2} . \ldots G_m^{dm} . \bmod n$$

Puis, les moyens de calcul et de comparaison du dispositif contrôleur vérifie que le message **M** et les défis **d** satisfont à la fonction de hachage

$$d = h(M, R')$$

• cas où le contrôleur dispose des engagements R et des réponses D

Dans le cas où le dispositif contrôleur dispose des engagements **R** et des réponses **D,** les moyens de calcul du dispositif contrôleur appliquent la fonction de hachage et calculent **d'** tel que

$$d' = h(M, R)$$

Puis, les moyens de calcul et de comparaison du dispositif contrôleur vérifient que les engagements **R**, les défis **d'** et les réponses **D**, satisfont à des relations du type :

$$R \equiv G_1^{d'1} . G_2^{d'2} . \ldots G_m^{d'm} . D^v \bmod n$$

ou à des relations du type :

$$R \equiv D^v / G_1^{d'1} . G_2^{d'2} . \ldots G_m^{d'm} . \bmod n$$

Cas où on choisit la valeur privée Q en premier et où on déduit la valeur publique G de la valeur privée Q

Dans certains, notamment afin de faciliter la production des couples de valeurs privées **Q** et publiques **G**, on choisit la valeur privée **Q** en premier et on déduit la valeur publique **G** de la valeur privée **Q**. Plus particulièrement dans ce cas, le système selon l'invention est tel que les composantes $Q_{i,1}$, $Q_{i,2}$, ... $Q_{i,f}$ des valeurs privées Q_i, sont des nombres tirés au hasard à raison d'une composante $Q_{i,j}$ ($Q_{i,j} \equiv Q_i \bmod p_j$) pour chacun desdits facteurs premiers p_j. Lesdites valeurs privées Q_i peuvent être calculées à partir desdites composantes $Q_{i,1}$, $Q_{i,2}$ ... $Q_{i,f}$ par la méthode des restes chinois. Lesdites valeurs publiques G_i, sont calculées en effectuant des opérations du type

$$G_{i,j} \equiv Q_{i,j}^v \bmod p_j$$

puis, en appliquant la méthode des restes chinois pour établir G_i tel que

$$G_i . Q_i^v \equiv 1 . \bmod n \text{ ou } G_i \equiv Q_i^v \bmod n ;$$

Ainsi, le nombre d'opérations arithmétiques modulo p_i à effectuer pour calculer chacun des $G_{i,j}$ pour chacun des p_j est réduit par rapport à ce qu'il

serait si les opérations étaient effectuées modulo **n**.

Avantageusement dans ce cas, le système selon l'invention est tel que l'exposant public de vérification **v** est un nombre premier. On démontre que la sécurité est équivalente à la connaissance de la valeur privée Q_i .

Cas où on choisit la valeur publique G en premier et où on déduit la valeur privée Q de la valeur publique G.

De préférence dans ce cas, ledit exposant **v** est tel que

$$v = 2^k$$

où **k** est un paramètre de sécurité plus grand que 1. Ladite valeur publique G_i est le carré g_i^2 d'un nombre de base g_i inférieur aux **f** facteurs premiers $p_1, p_2, \ldots p_f$. Le nombre de base g_i est tel que les deux équations :

$$x^2 \equiv g_i \bmod n \qquad \text{et} \qquad x^2 \equiv -g_i \bmod n$$

n'ont pas de solution en x dans l'anneau des entiers modulo **n** et tel que l'équation :

$$x^v \equiv g_i^2 \bmod n$$

a des solutions en x dans l'anneau des entiers modulo **n** .

Dispositif terminal

Méthode des restes chinois appliquée à la famille GQ

L'invention concerne aussi un dispositif terminal associé à une entité. Le dispositif terminal se présente notamment sous la forme d'un objet nomade par exemple sous la forme d'une carte bancaire à microprocesseur. Le dispositif terminal est destiné à prouver à dispositif contrôleur :

- l'authenticité d'une entité et/ou
- l'intégrité d'un message **M** associé à cette entité.

Cette preuve est établie au moyen de tout ou partie des paramètres suivants ou dérivés de ceux-ci:

- **m** couples de valeurs privées $Q_1, Q_2, \ldots Q_m$ et publiques $G_1, G_2, \ldots G_m$ (**m** étant supérieur ou égal à 1),
- un module public **n** constitué par le produit de **f** facteurs premiers

$p_1, p_2, \ldots p_f$ (f étant supérieur ou égal à 2),

- un exposant public **v** .

Ledit module, ledit exposant et lesdites valeurs sont liés par des relations du type :

$$G_i \cdot Q_i^v \equiv 1 \text{ . mod } n \text{ ou } G_i \equiv Q_i^v \text{ mod } n \text{ .}$$

Ledit dispositif terminal comprend un dispositif témoin comportant une zone mémoire contenant les **f** facteurs premiers p_i et/ou les paramètres des restes chinois des facteurs premiers et/ou du module public **n** et/ou les **m** valeurs privées Q_i et/ou les **f.m** composantes $Q_{i,j}$ ($Q_{i,j} \equiv Q_i \text{ mod } p_j$) des valeurs privées Q_i et de l'exposant public **v.** Le dispositif témoin comporte aussi :

- des moyens de production d'aléas, ci-après désignés les moyens de production d'aléas du dispositif témoin,

- des moyens de calcul, ci-après désignés les moyens de calcul des engagements **R** du dispositif témoin.

Les moyens de calcul permettent de calculer des engagements **R** dans l'anneau des entiers modulo **n.** Chaque engagement est calculé en effectuant des opérations du type

$$R_i \equiv r_i^v \text{ mod } p_i$$

où r_i est un aléa associé au nombre premier p_i tel que $0 < r_i < p_i$, chaque r_i appartenant à une collection d'aléas $\{r_1, r_2, \ldots r_f\}$ produits par les moyens de production d'aléas, puis en appliquant la méthode des restes chinois.

Ainsi, le nombre d'opérations arithmétiques modulo p_i à effectuer pour calculer chacun des engagements R_i pour chacun des p_i est réduit par rapport à ce qu'il serait si les opérations étaient effectuées modulo n.

Le dispositif témoin comporte aussi :

- des moyens de réception, ci-après désignés les moyens de réception des défis **d** du dispositif témoin, pour recevoir un ou plusieurs défis **d**, chaque défi **d** comportant **m** entiers d_i ci-après appelés défis élémentaires ;

- des moyens de calcul, ci-après désignés les moyens de calcul des réponses **D** du dispositif témoin, pour calculer à partir de chaque défi **d** une réponse **D** en effectuant des opérations du type :

$$D_i \equiv r_i \cdot Q_{i,1}^{d1} \cdot Q_{i,2}^{d2} \cdot \ldots Q_{i,m}^{dm} \bmod p_i$$

puis, en appliquant la méthode des restes chinois.

Ainsi, le nombre d'opérations arithmétiques modulo p_i à effectuer pour calculer chacune des réponses D_i pour chacun des p_i est réduit par rapport à ce qu'il serait si les opérations étaient effectuées modulo n.

Le dispositif témoin comporte aussi des moyens de transmission pour transmettre un ou plusieurs engagements **R** et une ou plusieurs réponses **D.** Il y a autant de réponses **D** que de défis **d** que d'engagements **R.** Chaque groupe de nombres **R, d, D** constituant un triplet noté **{R, d, D}.**

Cas de la preuve de l'authenticité d'une entité

Dans une première variante de réalisation, le dispositif terminal selon l'invention est destiné à prouver l'authenticité d'une entité appelée démonstrateur à une entité appelée contrôleur.

Ledit dispositif terminal est tel qu'il comporte un dispositif démonstrateur associé à l'entité démonstrateur. Ledit dispositif démonstrateur est interconnecté au dispositif témoin par des moyens d'interconnexion. Il peut se présenter notamment sous la forme de microcircuits logiques dans un objet nomade par exemple sous la forme d'un microprocesseur dans une carte bancaire à microprocesseur.

Ledit dispositif démonstrateur comporte des moyens de connexion pour le connecter électriquement, électromagnétiquement, optiquement ou de manière acoustique, notamment via un réseau de communication informatique, à un dispositif contrôleur associé à l'entité contrôleur. Ledit dispositif contrôleur se présente notamment sous la forme d'un terminal ou d'un serveur distant.

Ledit dispositif terminal permet d'exécuter les étapes suivantes :

• **étape 1 : acte d'engagement R**

A chaque appel, les moyens de calcul des engagements **R** du dispositif témoin calculent chaque engagement **R** en appliquant le processus spécifié ci-dessus.

Le dispositif témoin comporte des moyens de transmission, ci-après désignés les moyens de transmission du dispositif témoin, pour transmettre tout ou partie de chaque engagement **R** au dispositif démonstrateur, via les moyens d'interconnexion. Le dispositif démonstrateur comporte aussi des moyens de transmission, ci-après désignés les moyens de transmission du démonstrateur, pour transmettre tout ou partie de chaque engagement **R** au dispositif contrôleur, via les moyens de connexion.

• **étape 2 et 3 : acte de défi d, acte de réponse D**

Les moyens de réception des défis **d** du dispositif témoin, reçoivent chaque défi **d** provenant du dispositif contrôleur via les moyens de connexion entre le dispositif contrôleur et le dispositif démonstrateur et via les moyens d'interconnexion entre le dispositif démonstrateur et le dispositif témoin. Les moyens de calcul des réponses **D** du dispositif témoin calculent les réponses **D** à partir des défis **d** en appliquant le processus spécifié ci-dessus.

• **étape 4 : acte de contrôle**

Les moyens de transmission du démonstrateur transmettent chaque réponse **D** au dispositif contrôleur qui procède au contrôle.

Cas de la preuve de l'intégrité d'un message

Dans une deuxième variante de réalisation, susceptible d'être combinée aux autres variantes de réalisation, le dispositif terminal selon l'invention est destiné à prouver à une entité appelée contrôleur l'intégrité d'un message **M** associé à une entité appelée démonstrateur. Ledit dispositif terminal est tel qu'il comporte un dispositif démonstrateur associé à l'entité démonstrateur. Ledit dispositif démonstrateur est interconnecté au dispositif témoin par des moyens d'interconnexion. Il peut se présenter notamment sous la forme de

microcircuits logiques dans un objet nomade par exemple sous la forme d'un microprocesseur dans une carte bancaire à microprocesseur. Ledit dispositif démonstrateur comporte des moyens de connexion pour le connecter électriquement, électromagnétiquement, optiquement ou de manière acoustique, notamment via un réseau de communication informatique, à un dispositif contrôleur associé à l'entité contrôleur. Ledit dispositif contrôleur se présente notamment sous la forme d'un terminal ou d'un serveur distant.

Ledit dispositif terminal permet d'exécuter les étapes suivantes :

- **étape 1 : acte d'engagement R**

A chaque appel, les moyens de calcul des engagements **R** du dispositif témoin calculent chaque engagement **R** en appliquant le processus spécifié ci-dessus. Le dispositif témoin comporte des moyens de transmission, ci-après désignés les moyens de transmission du dispositif témoin, pour transmettre tout ou partie de chaque engagement **R** au dispositif démonstrateur, via les moyens d'interconnexion.

- **étape 2 et 3 : acte de défi d, acte de réponse**

Le dispositif démonstrateur comporte des moyens de calcul, ci-après désignés les moyens de calcul du dispositif démonstrateur, appliquant fonction de hachage **h** ayant comme arguments le message **M** et tout ou partie de chaque engagement **R** pour calculer au moins un jeton **T**. Le dispositif démonstrateur comporte aussi des moyens de transmission, ci-après désignés les moyens de transmission du démonstrateur, pour transmettre chaque jeton **T** , via les moyens de connexion, au dispositif au contrôleur.

Ledit dispositif contrôleur produit, après avoir reçu le jeton **T**, des défis **d** en nombre égal au nombre d'engagements **R**.

Les moyens de réception des défis **d** du dispositif témoin, reçoivent chaque défi **d** provenant du dispositif démonstrateur, via les moyens

d'interconnexion entre le dispositif démonstrateur et le dispositif témoin. Les moyens de calcul des réponses **D** du dispositif témoin calculent les réponses **D** à partir des défis **d** en appliquant le processus spécifié ci-dessus.

- **étape 4 : acte de contrôle**

Les moyens de transmission du démonstrateur transmettent chaque réponse **D** au dispositif contrôleur qui procède au contrôle.

Signature numérique d'un message et preuve de son authenticité

Opération de signature

Dans une troisième variante de réalisation, susceptible d'être combinée aux autres, le dispositif terminal selon l'invention est destiné à produire la signature numérique d'un message **M,** ci après désigné le message signé, par une entité appelée entité signataire.

Le message signé comprend :

- le message **M**,
- les défis **d** et/ou les engagements **R**,
- les réponses **D**.

Ledit dispositif terminal étant tel qu'il comporte un dispositif signataire associé à l'entité signataire. Ledit dispositif signataire est interconnecté au dispositif témoin par des moyens d'interconnexion. Il peut se présenter notamment sous la forme de microcircuits logiques dans un objet nomade par exemple sous la forme d'un microprocesseur dans une carte bancaire à microprocesseur. Ledit dispositif signataire comporte des moyens de connexion pour le connecter électriquement, électromagnétiquement, optiquement ou de manière acoustique, notamment via un réseau de communication informatique, à un dispositif contrôleur associé à l'entité contrôleur. Ledit dispositif contrôleur se présente notamment sous la forme d'un terminal ou d'un serveur distant.

Ledit dispositif terminal permet d'exécuter les étapes suivantes :

- **étape 1 : acte d'engagement R**

A chaque appel, les moyens de calcul des engagements **R** du dispositif témoin calculent chaque engagement **R** en appliquant le processus spécifié ci-dessus. Le dispositif témoin comporte des moyens de transmission, ci-après désignés les moyens de transmission du dispositif témoin, pour transmettre tout ou partie de chaque engagement **R** au dispositif signataire, via les moyens d'interconnexion.

- **étape 2 : acte de défi d**

Le dispositif signataire comporte des moyens de calcul, ci-après désignés les moyens de calcul du dispositif signataire, appliquant une fonction d hachage **h** ayant comme arguments le message **M** et tout ou partie de chaque engagement **R** pour calculer un train binaire et extraire de ce train binaire des défis **d** en nombre égal au nombre d'engagements **R.**

- **étape 3 : acte de réponse D**

Les moyens de réception des défis **d** reçoivent les défis **d** provenant du dispositif signataire, via les moyens d'interconnexion. Les moyens de calcul des réponses **D** du dispositif témoin calculent les réponses **D** à partir des défis **d** en appliquant le processus spécifié ci-dessus. Le dispositif témoin comporte des moyens de transmission, ci-après désignés les moyens de transmission du dispositif témoin, pour transmettre les réponses **D** au dispositif signataire, via les moyens d'interconnexion.

Dispositif contrôleur

Méthode des restes chinois appliquée à toute la famille GQ

L'invention concerne aussi un dispositif contrôleur. Le dispositif contrôleur peut se présenter notamment sous la forme d'un terminal ou d'un serveur distant associé à une entité contrôleur. Le dispositif contrôleur est destiné à prouver à un serveur contrôleur :

- l'authenticité d'une entité et/ou
- l'intégrité d'un message **M** associé à cette entité.

Cette preuve est établie au moyen de tout ou partie des paramètres suivants

ou dérivés de ceux-ci:

- **m** couples de valeurs privées $Q_1, Q_2, \ldots Q_m$ et publiques $G_1, G_2, \ldots G_m$ (**m** étant supérieur ou égal à 1),

- un module public **n** constitué par le produit de **f** facteurs premiers $p_1, p_2, \ldots p_f$ (**f** étant supérieur ou égal à 2),

- un exposant public **v** .

Ledit module, ledit exposant et lesdites valeurs sont liés par des relations du type :

$$G_i \cdot Q_i^v \equiv 1 \ . \bmod n \text{ ou } G_i \equiv Q_i^{-v} \bmod n \ ;$$

où Q_i désigne une valeur privée, inconnue du dispositif contrôleur, associée à la valeur publique G_i .

Cas de la preuve de l'authenticité d'une entité

Dans une première variante de réalisation, susceptible d'être combinée avec les autres, le dispositif contrôleur selon l'invention est destiné à prouver l'authenticité d'une entité appelée démonstrateur à une entité appelée contrôleur.

Ledit dispositif contrôleur comporte des moyens de connexion pour le connecter électriquement, électromagnétiquement, optiquement ou de manière acoustique, notamment via un réseau de communication informatique, à un dispositif démonstrateur associé à l'entité démonstrateur.

Ledit dispositif contrôleur permet d'exécuter les étapes suivantes :

- **étape 1 et 2 : acte d'engagement R, acte de défi**

Ledit dispositif contrôleur comporte aussi des moyens de réception de tout ou partie des engagements **R** provenant du dispositif démonstrateur, via les moyens de connexion.

Le dispositif contrôleur comporte des moyens de productions de défis pour produire, après avoir reçu tout ou partie de chaque engagement **R**, des défis **d** en nombre égal au nombre d'engagements **R**, chaque défi **d** comportant **m** entiers d_i , ci-après appelés défis élémentaires.

Le dispositif contrôleur comporte aussi des moyens de transmission, ci-après désignés les moyens de transmission du dispositif contrôleur, pour transmettre les défis **d** au démonstrateur, via les moyens de connexion.

• **étapes 3 et 4 : acte de réponse, acte de contrôle**

Le dispositif contrôleur comporte aussi

- des moyens de réception des réponses **D** provenant du dispositif démonstrateur, via les moyens de connexion,

- des moyens de calcul, ci-après désignés les moyens de calcul du dispositif contrôleur,

- des moyens de comparaison, ci-après désignés les moyens de comparaison du dispositif contrôleur.

Premier cas : le démonstrateur a transmis une partie de chaque engagement R

Dans le cas où les moyens de réception du dispositif contrôleur ont reçus une partie de chaque engagement **R**, les moyens de calcul du dispositif contrôleur, disposant des **m** valeurs publiques $G_1, G_2, \ldots G_m$, calculent à partir de chaque défi **d** et de chaque réponse **D** un engagement reconstruit **R'** satisfaisant à une relation du type :

$$R' \equiv G_1^{d1} . G_2^{d2} . \ldots G_m^{dm} . D^v \bmod n$$

ou à une relation du type,

$$R' \equiv D^v / G_1^{d1} . G_2^{d2} . \ldots G_m^{dm} . \bmod n .$$

Les moyens de comparaison du dispositif contrôleur comparent chaque engagement reconstruit **R'** à tout ou partie de chaque engagement **R** reçu.

Deuxième cas : le démonstrateur a transmis l'intégralité de chaque engagement R

Dans le cas où les moyens de réception du dispositif contrôleur ont reçus l'intégralité de chaque engagement **R**, les moyens de calcul et les moyens de comparaison du dispositif contrôleur, disposant des **m** valeurs publiques $G_1, G_2, \ldots G_m$, vérifient que chaque engagement **R** satisfait à une relation

du type :

$$R \equiv G_1^{d1} . G_2^{d2} . \ldots G_m^{dm} . D^v \bmod n$$

ou à une relation du type,

$$R \equiv D^v / G_1^{d1} . G_2^{d2} . \ldots G_m^{dm} . \bmod n .$$

Cas de la preuve de l'intégrité d'un message

Dans une deuxième variante de réalisation, susceptible d'être combinée avec les autres, le dispositif contrôleur selon l'invention est destiné à prouver l'intégrité d'un message **M** associé à une entité appelée démonstrateur.

Ledit dispositif contrôleur comporte des moyens de connexion pour le connecter électriquement, électromagnétiquement, optiquement ou de manière acoustique, notamment via un réseau de communication informatique, à un dispositif démonstrateur associé à l'entité démonstrateur. Ledit dispositif contrôleur permet d'exécuter les étapes suivantes :

- **étapes 1 et 2 : acte d'engagement R, acte de défi**

Ledit dispositif contrôleur comporte aussi des moyens de réception de jetons **T** provenant du démonstrateur, via les moyens de connexion. Le dispositif contrôleur comporte aussi des moyens de productions de défis pour produire, après avoir reçu le jeton **T**, défis **d** en nombre égal au nombre d'engagements **R** , chaque défi **d** comportant **m** entiers, ci-après appelés les défis élémentaires. Le dispositif contrôleur comporte aussi des moyens de transmission, ci-après désignés les moyens de transmission du dispositif contrôleur, pour transmettre les défis **d** au démonstrateur, via les moyens de connexion.

- **étapes 3 et 4 : acte de réponse D, acte de contrôle**

Le dispositif contrôleur comporte des moyens de réception des réponses **D** provenant du dispositif démonstrateur, via les moyens de connexion. Le dispositif contrôleur comporte aussi des moyens de calcul, ci-après désignés les moyens de calcul du dispositif contrôleur, disposant des **m** valeurs

publiques $G_1, G_2, \ldots G_m$, pour d'une part, calculer à partir de chaque défi **d** et de chaque réponse **D** un engagement reconstruit **R'** satisfaisant à une relation du type :

$$R' \equiv G_1^{d1} . G_2^{d2} . \ldots G_m^{dm} . D^v \bmod n$$

ou à une relation du type :

$$R' \equiv D^v / G_1^{d1} . G_2^{d2} . \ldots G_m^{dm} . \bmod n$$

puis d'autre part, calculer en appliquant la fonction de hachage **h** ayant comme arguments le message **M** et tout ou partie de chaque engagement reconstruit **R'**, un jeton **T'**.

Le dispositif contrôleur comporte aussi des moyens de comparaison, ci-après désignés les moyens de comparaison du dispositif contrôleur, pour comparer le jeton **T'** au jeton **T** reçu.

Signature numérique d'un message et preuve de son authenticité

Dans une troisième variante de réalisation, susceptible d'être combinée aux autres variantes de réalisation, le dispositif contrôleur selon l'invention est destiné à prouver l'authenticité du message **M** en contrôlant, par une entité appelée contrôleur, le message signé.

Le message signé, émis par un dispositif signataire associé à une entité signataire disposant d'une fonction de hachage **h (M, R)** ; comprend :

- le message **M**,
- les défis **d** et/ou les engagements **R**,
- les réponse **D** .

Ledit dispositif contrôleur comporte des moyens de connexion pour le connecter électriquement, électromagnétiquement, optiquement ou de manière acoustique, notamment via un réseau de communication informatique, à un dispositif signataire associé à l'entité signataire. Ledit dispositif contrôleur reçoit le message signé du dispositif signataire, via les moyens de connexion.

Le dispositif contrôleur comporte :

- des moyens de calcul, ci-après désignés les moyens de calcul du dispositif contrôleur,

- des moyens de comparaison, ci-après désignés les moyens de comparaison du dispositif contrôleur.

• cas où le contrôleur dispose des engagements R, des défis d, des réponses D,

Dans le cas où le dispositif contrôleur dispose des engagements **R**, des défis **d**, des réponses **D**, les moyens de calcul et de comparaison du dispositif contrôleur vérifient que les engagements **R**, les défis **d** et les réponses **D** satisfont à des relations du type

$$\mathbf{R \equiv G_1^{d1} . G_2^{d2} . \ldots G_m^{dm} . D^v \bmod n}$$

ou à des relations du type :

$$\mathbf{R \equiv D^v / G_1^{d1} . G_2^{d2} . \ldots G_m^{dm} . \bmod n}$$

Puis, les moyens de calcul et de comparaison du dispositif contrôleur vérifient que le message **M**, les défis **d** et les engagements **R** satisfont à la fonction de hachage

$$\mathbf{d = h (M, R)}$$

• cas où le contrôleur dispose des défis d et des réponses D

Dans le cas où le dispositif contrôleur dispose des défis **d** et des réponses **D**, les moyens de calcul du dispositif contrôleur calculent, à partir de chaque défi **d** et de chaque réponse **D**, des engagements **R'** satisfaisant à des relations du type :

$$\mathbf{R' \equiv G_1^{d1} . G_2^{d2} . \ldots G_m^{dm} . D^v \bmod n}$$

ou à des relations du type :

$$\mathbf{R' \equiv D^v / G_1^{d1} . G_2^{d2} . \ldots G_m^{dm} . \bmod n}$$

Puis, les moyens de calcul et de comparaison du dispositif contrôleur vérifient que le message **M** et les défis **d** satisfont à la fonction de hachage

$$\mathbf{d = h (M, R')}$$

• cas où le contrôleur dispose des engagements R et des réponses D

Dans le cas où le dispositif contrôleur dispose des engagements **R** et des réponses **D,** les moyens de calcul du dispositif contrôleur appliquent la fonction de hachage et calculent **d'** tel que

$$d' = h(M, R)$$

Puis, les moyens de calcul et de comparaison du dispositif contrôleur vérifient que les engagements **R**, les défis **d'** et les réponses **D**, satisfont à des relations du type :

$$R \equiv G_1^{d'1} . G_2^{d'2} . \ldots G_m^{d'm} . D^v \bmod n$$

ou à des relations du type :

$$R \equiv D^v / G_1^{d'1} . G_2^{d'2} . \ldots G_m^{d'm} . \bmod n$$

Description détaillée de la variante de réalisation dans le cas où l'exposant public $v = 2^k$

Description

Rappelons l'objectif de la technologie GQ : l'authentification dynamique d'entités et de messages associés, ainsi que la signature numérique de messages.

La version classique de la technologie GQ fait appel à la technologie RSA. Mais, si la technologie RSA dépend bel et bien de la factorisation, cette dépendance n'est pas une équivalence, loin s'en faut, comme le démontrent les attaques dites « multiplicatives » contre diverses normes de signature numérique mettant en œuvre la technologie RSA.

Dans le cadre de la technologie GQ2, la présente partie de l'invention porte plus précisément sur l'utilisation des jeux de clés GQ2 dans le cadre de l'authentification dynamique et de la signature numérique. La technologie GQ2 ne fait pas appel à la technologie RSA. L'objectif est double : d'une part, améliorer les performances par rapport à la technologie RSA ; d'autre part, éviter les problèmes inhérents à la technologie RSA. La clé privée GQ2 est la factorisation du module n. Toute attaque au niveau de striplets GQ2 se ramène à la factorisation du module n : il y a cette fois équivalence. Avec la technologie GQ2, la charge de travail est réduite, tant pour l'entité qui signe ou qui s'authentifie que pour celle qui contrôle. Grâce à un meilleur usage du problème de la factorisation, tant en sécurité qu'en performance, la technologie GQ2 concurrence la technologie RSA.

La technologie GQ2 utilise un ou plusieurs petits nombres entiers plus grands que 1, disons m petits nombres entiers ($m \geq 1$) appelés « nombres de base » et notés par g_i. Les nombres de base étant fixés de g_1 à g_m avec $m \geq 1$, une clé publique de vérification $\langle v, n \rangle$ est choisie de la manière suivante. L'exposant public de vérification v est 2^k où k est un petit nombre entier plus grand que 1 ($k \geq 2$). Le module public n est le produit d'au moins deux facteurs premiers plus grands que les nombres de base, disons f facteurs premiers ($f \geq 2$) notés par p_j, de $p_1 \ldots p_f$. Les f facteurs premiers

sont choisis de façon à ce que le module public n ait les propriétés suivantes par rapport à chacun des m nombres de base de g_1 à g_m.

- D'une part, les équations (1) et (2) n'ont pas de solution en x dans l'anneau des entiers modulo n, c'est-à-dire que g_i et $-g_i$ sont deux résidus non quadratiques (mod n).

$$x^2 \equiv g_i \pmod{n} \qquad (1)$$

$$x^2 \equiv -g_i \pmod{n} \qquad (2)$$

- D'autre part, l'équation (3) a des solutions en x dans l'anneau des entiers modulo n.

$$x^{2^k} \equiv g_i^2 \pmod{n} \qquad (3)$$

La clé publique de vérification $\langle v, n \rangle$ étant fixée selon les nombres de base de g_1 à g_m avec $m \geq 1$, chaque nombre de base g_i détermine un couple de valeurs GQ2 comprenant une valeur publique G_i et une valeur privée Q_i: soit m couples notés de G_1 Q_1 à G_m Q_m. La valeur publique G_i est le carré du nombre de base g_i: soit $G_i = g_i^2$. La valeur privée Q_i est une des solutions à l'équation (3) ou bien l'inverse (mod n) d'une telle solution.

De même que le module n se décompose en f facteurs premiers, l'anneau des entiers modulo n se décompose en f corps de Galois, de CG(p_1) à CG(p_f). Voici les projections des équations (1), (2) et (3) dans CG(p_j).

$$x^2 \equiv g_i \pmod{p_j} \qquad (1.a)$$

$$x^2 \equiv -g_i \pmod{p_j} \qquad (2.a)$$

$$x^{2^k} \equiv g_i^2 \pmod{p_j} \qquad (3.a)$$

Chaque valeur privée Q_i peut se représenter de manière unique par f composantes privées, une par facteur premier : $Q_{i,j} \equiv Q_i \pmod{p_j}$. Chaque composante privée $Q_{i,j}$ est une solution à l'équation (3.a) ou bien l'inverse (mod p_j) d'une telle solution. Après que toutes les solutions possibles à chaque équation (3.a) aient été calculées, la technique des restes chinois permet d'établir toutes les valeurs possibles pour chaque valeur privée Q_i à partir de f composantes de $Q_{i,1}$ à $Q_{i,f}$: Q_i = Restes Chinois ($Q_{i,1}$, $Q_{i,2}$, ... $Q_{i,f}$)

de manière à obtenir toutes les solutions possibles à l'équation (3).

Voici la technique des restes chinois : soient deux nombres entiers positifs premiers entre eux a et b tels que $0 < a < b$, et deux composantes X_a de 0 à $a-1$ et X_b de 0 à $b-1$; il s'agit de déterminer X = Restes Chinois (X_a, X_b), c'est-à-dire, le nombre unique X de 0 à $a.b-1$ tel que $X_a \equiv X \pmod{a}$ et $X_b \equiv X \pmod{b}$. Voici le paramètre des restes chinois : $\alpha \equiv \{b \pmod{a}\}^{-1} \pmod{a}$. Voici l'opération des restes chinois : $\varepsilon \equiv X_b \pmod{a}$; $\delta = X_a - \varepsilon$; si δ est négatif, remplacer δ par $\delta + a$; $\gamma \equiv \alpha \,.\, \delta \pmod{a}$; $X = \gamma \,.\, b + X_b$.

Lorsque les facteurs premiers sont rangés dans l'ordre croissant, du plus petit p_1 au plus grand p_f, les paramètres des restes chinois peuvent être les suivants (il y en a $f-1$, c'est-à-dire, un de moins que de facteurs premiers). Le premier paramètre des restes chinois est $\alpha \equiv \{p_2 \pmod{p_1}\}^{-1} \pmod{p_1}$. Le second paramètre des restes chinois est $\beta \equiv \{p_1.p_2 \pmod{p_3}\}^{-1} \pmod{p_3}$. Le i ième paramètre des restes chinois est $\lambda \equiv \{p_1.p_2. \ldots p_{i-1} \pmod{p_i}\}^{-1} \pmod{p_i}$. Et ainsi de suite. Ensuite, en $f-1$ opérations des restes chinois, on établit un premier résultat (mod p_2 fois p_1) avec le premier paramètre, puis, un second résultat (mod $p_1.p_2$ fois p_3) avec le second paramètre, et ainsi de suite, jusqu'à un résultat (mod $p_1. \ldots p_{f-1}$ fois p_f), c'est-à-dire, (mod n).

Il y a plusieurs représentations possibles de la clé privée GQ2, ce qui traduit **le polymorphisme de la clé privée GQ2.** Les diverses représentations s'avèrent équivalentes : elles se ramènent toutes à la connaissance de la factorisation du module n qui est la véritable clé privée GQ2. Si la représentation affecte bien le comportement de l'entité qui signe ou qui s'authentifie, elle n'affecte pas le comportement de l'entité qui contrôle.

Voici les trois principales représentations possibles de la clé privée GQ2.

1) La représentation classique en technologie GQ consiste à stocker m valeurs privées Q_i et la clé publique de vérification $\langle v, n \rangle$; en technologie GQ2, cette représentation est concurrencée par les deux suivantes. 2) La représentation optimale en termes de charges de travail consiste à stocker

l'exposant public v, les f facteurs premiers p_j, $m.f$ composantes privées $Q_{i,j}$ et f–1 paramètres des restes chinois. 3) La représentation optimale en termes de taille de clé privée consiste à stocker l'exposant public v, les m nombres de base g_i et les f facteurs premiers p_j, puis, à commencer chaque utilisation en établissant ou bien m valeurs privées Q_i et le module n pour se ramener à la première représentation, ou bien $m.f$ composantes privées $Q_{i,j}$ et f–1 paramètres des restes chinois pour se ramener à la seconde.

Les entités qui signent ou s'authentifient peuvent toutes utiliser les mêmes nombres de base ; sauf contre indication, les m nombres de base de g_1 à g_m peuvent alors avantageusement être les m premiers nombres premiers.

Parce que la sécurité du mécanisme d'authentification dynamique ou de signature numérique équivaut à la connaissance d'une décomposition du module, la technologie GQ2 ne permet pas de distinguer simplement deux entités utilisant le même module. Généralement, chaque entité qui s'authentifie ou signe dispose de son propre module GQ2. Toutefois, on peut spécifier des modules GQ2 à quatre facteurs premiers dont deux sont connus d'une entité et les deux autres d'une autre.

Voici un premier jeu de clés GQ2 avec $\boldsymbol{k = 6}$, soit $v = 64$, $\boldsymbol{m = 3}$, soit trois nombres de base : $g_1 = 3$, $g_2 = 5$ et $g_3 = 7$, et $\boldsymbol{f = 3}$, soit un module à trois facteurs premiers : deux congrus à 3 (mod 4) et un à 5 (mod 8). Notons que $g = 2$ est incompatible avec un facteur premier congru à 5 (mod 8).

p_1 = 03CD2F4F21E0EAD60266D5CFCEBB6954683493E2E833

p_2 = 0583B097E8D8D777BAB3874F2E76659BB614F985EC1B

p_3 = 0C363CD93D6B3FEC78EE13D7BE9D84354B8FDD6DA1FD

$n = p_1 . p_2 . p_3$ = FFFF81CEA149DCF2F72EB449C5724742FE2A3630D9
02CC00EAFEE1B957F3BDC49BE9CBD4D94467B72AF28CFBB26144
CDF4BBDBA3C97578E29CC9BBEE8FB6DDDD

$Q_{1,1}$ = 0279C60D216696CD6F7526E23512DAE090CFF879FDDE

$Q_{2,1}$ = 7C977FC38F8413A284E9CE4EDEF4AEF35BF7793B89

$Q_{3,1}$ = 6FB3B9C05A03D7CADA9A3425571EF5ECC54D7A7B6F

$Q_{1,2}$ = 0388EC6AA1E87613D832E2B80E5AE8C1DF2E74BFF502

$Q_{2,2}$ = 04792CE70284D16E9A158C688A7B3FEAF9C40056469E

$Q_{3,2}$ = FDC4A8E53E185A4BA793E93BEE5C636DA731BDCA4E

$Q_{1,3}$ = 07BC1AB048A2EAFDAB59BD40CCF2F657AD8A6B573BDE

$Q_{2,3}$ = 0AE8551E116A3AC089566DFDB3AE003CF174FC4E4877

$Q_{3,3}$ = 01682D490041913A4EA5B80D16B685E4A6DD88070501

Q_1 = D7E1CAF28192CED6549FF457708D50A7481572DD5F2C335D8
C69E22521B510B64454FB7A19AEC8D06985558E764C6991B05FC2A
C74D9743435AB4D7CF0FF6557

Q_2 = CB1ED6B1DD649B89B9638DC33876C98AC7AF689E9D1359E4
DB17563B9B3DC582D5271949F3DBA5A70C108F561A274405A5CB8
82288273ADE67353A5BC316C093

Q_3 = 09AA6F4930E51A70CCDFA77442B10770DD1CD77490E3398A
AD9DC50249C34312915E55917A1ED4D83AA3D607E3EB5C8B197
697238537FE7A0195C5E8373EB74D

Voici un second jeu de clés GQ2, avec $k = 9$, soit $v = 512$, $m = 2$, soit deux nombres de base : $g_1 = 2$ et $g_2 = 3$, et $f = 3$, soit un module à trois facteurs premiers congrus à 3 (mod 4).

p_1 = 03852103E40CD4F06FA7BAA9CC8D5BCE96E3984570CB

p_2 = 062AC9EC42AA3E688DC2BC871C8315CB939089B61DD7

p_3 = 0BCADEC219F1DFBB8AB5FE808A0FFCB53458284ED8E3

$n = p_1 . p_2 . p_3$ = FFFF5401ECD9E537F167A80C0A9111986F7A8EBA4D
6698AD68FF670DE5D9D77DFF00716DC7539F7CBBCF969E73A0C49
761B276A8E6B6977A21D51669D039F1D7

$Q_{1,1}$ = 0260BC7243C22450D566B5C6EF74AA29F2B927AF68E1

$Q_{2,1}$ = 0326C12FC7991ECDC9BB8D7C1C4501BE1BAE9485300E

$Q_{1,2}$ = 02D0B4CC95A2DD435D0E22BFBB29C59418306F6CD00A

$Q_{2,2}$ = 045ECB881387582E7C556887784D2671CA118E22FCF2

$Q_{1,3}$ = B0C2B1F808D24F6376E3A534EB555EF54E6AEF5982

$Q_{2,3}$ = 0AB9F81DF462F58A52D937E6D81F48FFA4A87A9935AB

Q_1 = 27F7B9FC82C19ACAE47F3FE9560C3536A7E90F8C3C51E13C
35F32FD8C6823DF753685DD63555D2146FCDB9B28DA367327DD6
EDDA092D0CF108D0AB708405DA46

Q_2 = 230D0B9595E5AD388F1F447A69918905EBFB05910582E5BA64
9C94B0B2661E49DF3C9B42FEF1F37A7909B1C2DD54113ACF87C6
F11F19874DE7DC5D1DF2A9252D

Authentification dynamique

Le mécanisme d'authentification dynamique est destiné à prouver à une entité appelée **contrôleur** l'authenticité d'une autre entité appelée **démonstrateur** ainsi que l'authenticité d'un éventuel message associé *M*, de sorte que le contrôleur s'assure qu'il s'agit bien du démonstrateur et éventuellement que lui et le démonstrateur parlent bien du même message *M*. Le message associé *M* est optionnel, ce qui signifie qu'il peut être vide.

Le mécanisme d'authentification dynamique est une séquence de quatre actes : un acte d'engagement, un acte de défi, un acte de réponse et un acte de contrôle. Le démonstrateur joue les actes d'engagement et de réponse. Le contrôleur joue les actes de défi et de contrôle.

Au sein du démonstrateur, on peut isoler un témoin, de manière à isoler les paramètres et les fonctions les plus sensibles du démonstrateur, c'est-à-dire, la production des engagements et des réponses. Le témoin dispose du paramètre *k* et de la clé privée GQ2, c'est-à-dire, de la factorisation du module *n* selon l'une des trois représentations évoquées ci-dessus : • les *f* facteurs premiers et les *m* nombres de base, • les *m.f* composantes privées, les *f* facteurs premiers et *f*–1 paramètres des restes chinois, • les *m* valeurs privées et le module *n*.

Le témoin peut correspondre à une réalisation particulière, par exemple, • une carte à puce reliée à un PC formant ensemble le démonstrateur, ou

encore, • des programmes particulièrement protégés au sein d'un PC, ou encore, • des programmes particulièrement protégés au sein d'une carte à puce. Le témoin ainsi isolé est semblable au témoin défini ci-après au sein du signataire. A chaque exécution du mécanisme, le témoin produit un ou plusieurs engagements R, puis, autant de réponses D à autant de défis d. Chaque ensemble $\{R, d, D\}$ constitue un **triplet GQ2**.

Outre qu'il comprend le témoin, le démonstrateur dispose également, le cas échéant, d'une fonction de hachage et d'un message M.

Le contrôleur dispose du module n et des paramètres k et m ; le cas échéant, il dispose également de la même fonction de hachage et d'un message M'. Le contrôleur est apte à reconstituer un engagement R' à partir de n'importe quel défi d et de n'importe quelle réponse D. Les paramètres k et m renseignent le contrôleur. Faute d'indication contraire, les m nombres de base de g_1 à g_m sont les m premiers nombres premiers. Chaque défi d doit comporter m défis élémentaires notés de d_1 à d_m : un par nombre de base. Chaque défi élémentaire de d_1 à d_m doit prendre une valeur de 0 à $2^{k-1}-1$ (les valeurs de $v/2$ à $v-1$ ne sont pas utilisées). Typiquement, chaque défi est codé par m fois $k-1$ bits (et non pas m fois k bits). Par exemple, avec $k = 6$ et $m = 3$ et les nombres de base 3, 5 et 7, chaque défi comporte 15 bits transmis sur deux octets ; avec $k = 9$, $m = 2$ et les nombres de base 2 et 3, chaque défi comporte 16 bits transmis sur deux octets. Lorsque les $(k-1).m$ défis possibles sont également probables, la valeur $(k-1).m$ détermine la sécurité apportée par chaque triplet GQ2 : un imposteur qui, par définition, ne connaît pas la factorisation du module n a exactement une chance de succès sur $2^{(k-1).m}$. Lorsque $(k-1).m$ vaut de 15 à 20, un triplet suffit à assurer raisonnablement l'authentification dynamique. Pour atteindre n'importe quel niveau de sécurité, on peut produire des triplets en parallèle ; on peut également en produire en séquence, c'est-à-dire, répéter l'exécution du mécanisme.

1) L'acte d'engagement comprend les opérations suivantes.

Lorsque le témoin dispose des m valeurs privées de Q_1 à Q_m et du module n, il tire au hasard et en privé un ou plusieurs aléas r ($0 < r < n$) ; puis, par k élévations successives au carré (mod n), il transforme chaque aléa r en un engagement R.

$$R \equiv r^v \pmod{n}$$

Voici un exemple avec le premier jeu de clés avec $k = 6$.

r = B8AD426C1AC0165E94B894AC2437C1B1797EF562CFA53A4AF8
43131FF1C89CFDA131207194710EF9C010E8F09C60D9815121981260
919967C3E2FB4B4566088E

R = FFDD736B666F41FB771776D9D50DB7CDF03F3D976471B25C56
D3AF07BE692CB1FE4EE70FA77032BECD8411B813B4C21210C6B04
49CC4292E5DD2BDB00828AF18

Lorsque le témoin dispose des f facteurs premiers de p_1 à p_f et des mf composantes privées Q_{ij}, il tire au hasard et en privé une ou plusieurs collections de f aléas : chaque collection comporte un aléa r_i par facteur premier p_i ($0 < r_i < p_i$) ; puis, par k élévations successives au carré (mod p_i), il transforme chaque aléa r_i en une composante d'engagement R_i.

$$R_i \equiv r_i^v \pmod{p_i}$$

Voici un exemple avec le second jeu de clés avec $k = 9$.

r_1 = B0418EABEBADF0553A28903F74472CD49EE8C82D86

R_1 = 022B365F0BEA8E157E94A9DEB0512827FFD5149880F1

r_2 = 75A8DA8FE0E60BD55D28A218E31347732339F1D667

R_2 = 057E43A242C485FC20DEEF291C774CF1B30F0163DEC2

r_3 = 0D74D2BDA5302CF8BE2F6D406249D148C6960A7D27

R_3 = 06E14C8FC4DD312BA3B475F1F40CF01ACE2A88D5BB3C

Pour chaque collection de f composantes d'engagement, le témoin établit un engagement selon la technique des restes chinois. Il y a autant d'engagements que de collections d'aléas.

$$R = \text{Restes Chinois}(R_1, R_2, \ldots R_f)$$

R = 28AA7F12259BFBA81368EB49C93EEAB3F3EC6BF73B0EBD7
D3FC8395CFA1AD7FC0F9DAC169A4F6F1C46FB4C3458D1E37C9
9123B56446F6C928736B17B4BA4A529

Dans les deux cas, le démonstrateur transmet au contrôleur tout ou partie de chaque engagement $\boldsymbol{R}$, ou bien, un code de hachage $\boldsymbol{H}$ obtenu en hachant chaque engagement $\boldsymbol{R}$ et un message $\boldsymbol{M}$.

2) L'acte de défi consiste à tirer au hasard un ou plusieurs défis d composés chacun de m défis élémentaires $d_1\ d_2\ \ldots\ d_m$; chaque défi élémentaire d_i prend l'une des valeurs de 0 à $v/2-1$.

$$d = d_1\ d_2 \ldots\ d_m$$

Voici un exemple pour le premier jeu de clés avec $k = 6$ et $m = 3$.

$$d_1 = 10110 = 22 = \text{'16'}\ ;\ d_2 = 00111 = 7\ ;\ d_3 = 00010 = 2,$$

$$d = 0 \,||\, d_1 \,||\, d_2 \,||\, d_3 = 01011000\ 11100010 = 58\ \text{E2}$$

Voici un exemple pour le second jeu de clés avec $k = 9$ et $m = 2$.

$$d = d_1 \,||\, d_2 = 58\ \text{E2} = \text{soit en décimal, 88 et 226}$$

Le contrôleur transmet au démonstrateur chaque défi $\boldsymbol{d}$.

3) L'acte de réponse comporte les opérations suivantes.

Lorsque le témoin dispose des m valeurs privées de Q_1 à Q_m et du module n, il calcule une ou plusieurs réponses D en utilisant chaque aléa r de l'acte d'engagement et les valeurs privées selon les défis élémentaires.

$$X \equiv Q_1^{d_1}.Q_2^{d_2}...Q_m^{d_m} \pmod{n}$$

$$D \equiv r.X \pmod{n}$$

Voici un exemple pour le premier jeu de clés.

D = FF257422ECD3C7A03706B9A7B28EE3FC3A4E974AEDCDF386
5EEF38760B859FDB5333E904BBDD37B097A989F69085FE8EF6480
A2C6A290273479FEC9171990A17

Lorsque le témoin dispose des f facteurs premiers de p_1 à p_f et des $m.f$ composantes privées Q_{ij}, il calcule une ou plusieurs collections de f

composantes de réponse en utilisant chaque collection d'aléas de l'acte d'engagement : chaque collection de composantes de réponse comporte une composante par facteur premier.

$$X_i \equiv Q_{1,i}^{d_1} . Q_{2,i}^{d_2} ... Q_{m,i}^{d_m} \pmod{p_i}$$

$$D_i \equiv r_i . X_i \pmod{p_i}$$

Voici un exemple pour le second jeu de clés.

$D_1 = r_1 \cdot Q_{1,1}^{d1} \cdot Q_{2,1}^{d2} \pmod{p_1} =$

02660ADF3C73B6DC15E196152322DDE8EB5B35775E38

$D_2 = r_2 \cdot Q_{1,2}^{d1} \cdot Q_{2,2}^{d2} \pmod{p_2} =$

04C15028E5FD1175724376C11BE77052205F7C62AE3B

$D_3 = r_3 \cdot Q_{1,3}^{d1} \cdot Q_{2,3}^{d2} \pmod{p_3} =$

0903D20D0C306C8EDA9D8FB5B3BEB55E061AB39CCF52

Pour chaque collection de composantes de réponse, le témoin établit une réponse selon la technique des restes chinois. Il y a autant de réponses que de défis.

$$D = \text{Restes Chinois}(D_1, D_2, \ldots D_f)$$

D = 85C3B00296426E97897F73C7DC6341FB8FFE6E879AE12EF1F36

4CBB55BC44DEC437208CF530F8402BD9C511F5FB3B3A309257A00

195A7305C6FF3323F72DC1AB

Dans les deux cas, le démonstrateur transmet chaque réponse D au contrôleur.

4) L'acte de contrôle consiste à contrôler que chaque triplet $\{R, d, D\}$ vérifie une équation du type suivant pour une valeur non nulle,

$$R . \prod_{i=1}^{m} G_i^{d_i} \equiv D^{2^k} \pmod{n} \quad \text{ou bien} \quad R \equiv D^{2^k} . \prod_{i=1}^{m} G_i^{d_i} \pmod{n}$$

ou bien, à rétablir chaque engagement : aucun ne doit être nul.

$$- \; R' \equiv D^{2^k} / \prod_{i=1}^{m} G_i^{d_i} \pmod{n} \quad \text{ou bien} \quad R' \equiv D^{2^k} . \prod_{i=1}^{m} G_i^{d_i} \pmod{n}$$

Eventuellement, le contrôleur calcule ensuite un code de hachage H' en

hachant chaque engagement rétabli R' et un message M'. L'authentification dynamique est réussie lorsque le contrôleur retrouve ainsi ce qu'il a reçu à l'issue de l'acte d'engagement, c'est-à-dire, tout ou partie de chaque engagement R, ou bien, le code de hachage H.

Par exemple, une séquence d'opérations élémentaires transforme la réponse D en un engagement R'. La séquence comprend k carrés (mod n) séparés par k–1 divisions ou multiplications (mod n) par des nombres de base. Pour la i ième division ou multiplication, qui s'effectue entre le i ième carré et le i+1 ième carré, le i ième bit du défi élémentaire d_1 indique s'il faut utiliser g_1, le i ième bit du défi élémentaire d_2 indique s'il faut utiliser g_2, ... jusqu'au i ième bit du défi élémentaire d_m qui indique s'il faut utiliser g_m.

Voici un exemple pour le premier jeu de clés.

D^2 (mod n) =

FD12E8E1F1370AEC9C7BA2E05C80AD2B692D341D46F3
2B93948715491F0EB091B7606CA1E744E0688367D7BB998F7B73D5F7
FDA95D5BD6347DC8B978CA217733

$3 . D^2$ (mod n) = F739B708911166DFE715800D8A9D78FC3F332FF622D
3EAB8E7977C68AD44962BEE4DAE3C0345D1CB34526D3B67EBE8BF
987041B4852890D83FC6B48D3EF6A9DF

$3^2 . D^4$ (mod n) = 682A7AF280C49FE230BEE354BF6FFB30B7519E3C8
92DD07E5A781225BBD33920E5ADABBCD7284966D71141EAA17AF
8826635790743EA7D9A15A33ACC7491D4A7

$3^4 . D^8$ (mod n) = BE9D828989A2C184E34BA8FE0F384811642B7B548F
870699E7869F8ED851FC3DB3830B2400C516511A0C28AFDD210EC3
939E69D413F0BABC6DEC441974B1A291

$3^5 . 5 . D^8$ (mod n) = 2B40122E225CD858B26D27B768632923F2BBE5
DB15CA9EFA77EFA667E554A02AD1A1E4F6B59BD9E1AE4A537D
4AC1E89C2235C363830EBF4DB42CEA3DA98CFE00

$3^{10} . 5^2 . D^{16}$ (mod n) =

BDD3B34C90ABBC870C604E27E7F2E9DB2D383
68EA46C931C66F6C7509B118E3C162811A98169C30D4DEF768397DD
B8F6526B6714218DEB627E11FACA4B9DB268

$3^{11} . 5^3 . 7 . D^{16} \pmod{n} =$
DBFA7F40D338DE4FBA73D42DBF427BBF195
C13D02AB0FA5F8C8DDB5025E34282311CEF80BACDCE5D0C433444
A2AF2B15318C36FE2AE02F3C8CB25637C9AD712F

$3^{22} . 5^6 . 7^2 . D^{32} \pmod{n}$ = C60CA9C4A11F8AA89D9242CE717E3DC6C1
A95D5D09A2278F8FEE1DFD94EE84D09D000EA8633B53C4A0E7F0A
EECB70509667A3CB052029C94EDF27611FAE286A7

$3^{22} . 5^7 . 7^2 . D^{32} \pmod{n} =$
DE40CB6B41C01E722E4F312AE7205F18CDD
0303EA52261CB0EA9F0C7E0CD5EC53D42E5CB645B6BB1A3B00C77
886F4AC5222F9C863DACA440CF5F1A8E374807AC

$3^{44} . 5^{14} . 7^4 . D^{64} \pmod{n}$, c'est-à-dire, $3^{2C} . 5^E . 7^4 . D^{40} \pmod{n}$ avec les exposants en hexa = FFDD736B666F41FB771776D9D50DB7CDF03F3D9
76471B25C56D3AF07BE692CB1FE4EE70FA77032BECD8411B813B4C
21210C6B0449CC4292E5DD2BDB00828AF18

On retrouve bien l'engagement ***R***. L'authentification est réussie.

Voici un exemple pour le second jeu de clés.

$D^2 \pmod{n}$ = C66E585D8F132F7067617BC6D00BA699ABD74FB9D13E
24E6A6692CC8D2FC7B57352D66D34F5273C13F20E3FAA228D70AEC
693F8395ACEF9206B172A8A2C2CCBB

$3 . D^2 \pmod{n}$ = 534C6114D385C3E15355233C5B00D09C2490D1B8D8E
D3D59213CB83EAD41C309A187519E5F501C4A45C37EB2FF38FBF20
1D6D138F3999FC1D06A2B2647D48283

$3^2 . D^4 \pmod{n}$ = A9DC8DEA867697E76B4C18527DFFC49F4658473D03
4EC1DDE0EB21F6F65978BE477C4231AC9B1EBD93D5D49422408E47
15919023B16BC3C6C46A92BBD326AADF

$2 . 3^3 . D^4 \pmod n$ = FB2D57796039DFC4AF9199CAD44B66F257A1FF
3F2BA4C12B0A8496A0148B4DFBAFE838E0B5A7D9FB4394379D72A
107E45C51FCDB7462D03A35002D29823A2BB5

$2^2 . 3^6 . D^8 \pmod n$ = 4C210F96FF6C77541910623B1E49533206DFB9E91
6521F305F12C5DB054D4E1BF3A37FA293854DF02B49283B6DE5E5D
82ACB23DAF1A0D5A721A1890D03A00BD8

$2^2 . 3^7 . D^8 \pmod n$ = E4632EC4FE4565FC4B3126B15ADBF996149F2D
BB42F65D911D3851910FE7EA53DAEA7EE7BA8FE9D081DB78B249
B1B18880616B90D4E280F564E49B270AE02388

$2^4 . 3^{14} . D^{16} \pmod n$ = ED3DDC716AE3D1EA74C5AF935DE814BCC
2C78B12A6BB29FA542F9981C5D954F53D153B9F0198BA82690EF
665C17C399607DEA54E218C2C01A890D422EDA16FA3

$2^5 . 3^{14} . D^{16} \pmod n$ =
DA7C64E0E8EDBE9CF823B71AB13F17E1161487
6B000FBB473F5FCBF5A5D8D26C7B2A05D03BDDD588164E562D0F5
7AE94AE0AD3F35C61C0892F4C91DC0B08ED6F

$2^{10} . 3^{28} . D^{32} \pmod n$ = 6ED6AFC5A87D2DD117B0D89072C99FB9DC9
5D558F65B6A1967E6207D4ADBBA32001D3828A35069B256A07C3D
722F17DA30088E6E739FBC419FD7282D16CD6542

$2^{11} . 3^{28} . D^{32} \pmod n$ = DDAD5F8B50FA5BA22F61B120E5933F73B92
BAAB1ECB6D432CFCC40FA95B77464003A705146A0D364AD40F8
7AE45E2FB460111CDCE73F78833FAE505A2D9ACA84

$2^{22} . 3^{56} . D^{64} \pmod n$ = A466D0CB17614EFD961000BD9EABF4F021
36F8307101882BC1764DBAACB715EFBF5D8309AE001EB5DEDA
8F000E44B3D4578E5CA55797FD4BD1F8E919BE787BD0

$2^{44} . 3^{112} . D^{128} \pmod n$ = 925B0EDF5047EFEC5AFABDC03A830919761
B8FBDD2BF934E2A8A31E29B976274D513007EF1269E4638B4F65F
8FDEC740778BDC178AD7AF2968689B930D5A2359

$2^{44} . 3^{113} . D^{128} \pmod n$ = B711D89C03FDEA8D1F889134A4F809B3F2D

8207F2AD8213D169F2E99ECEC4FE08038900F0C203B55EE4F4C803
BFB912A04F11D9DB9D076021764BC4F57D47834

$2^{88} \cdot 3^{226} \cdot D^{256} \pmod{n} =$
41A83F119FFE4A2F4AC7E5597A5D0BEB4D4C
08D19E597FD034FE720235894363A19D6BC5AF323D24B1B7FCFD8D
FCC628021B4648D7EF757A3E461EF0CFF0EA13

$2^{176} \cdot 3^{452} \cdot D^{512} \pmod{n}$, soit $4^{88} \cdot 9^{226} \cdot D^{512} \pmod{n} =$
28AA7F12259BFBA8
1368EB49C93EEAB3F3EC6BF73B0EBD7D3FC8395CFA1AD7FC0F9D
AC169A4F6F1C46FB4C3458D1E37C99123B56446F6C928736B17B4BA
4A529

On retrouve bien l'engagement R. L'authentification est réussie.

Signature numérique

Le mécanisme de signature numérique permet à une entité appelée **signataire** de produire des messages signés et à une entité appelée **contrôleur** de vérifier des messages signés. Le message M est une séquence binaire quelconque : il peut être vide. Le message M est signé en lui adjoignant un appendice de signature qui comprend un ou plusieurs engagements et / ou défis, ainsi que les réponses correspondantes.

Le contrôleur dispose de la même fonction de hachage, des paramètres k et m et du module n. Les paramètres k et m renseignent le contrôleur. D'une part, chaque défi élémentaire, de d_1 à d_m, doit prendre une valeur de 0 à $2^{k-1}-1$ (les valeurs de $v/2$ à $v-1$ ne sont pas utilisées). D'autre part, chaque défi d doit comporter m défis élémentaires notés de d_1 à d_m, autant que de nombres de base. En outre, faute d'indication contraire, les m nombres de base, de g_1 à g_m, sont les m premiers nombres premiers. Avec $(k-1).m$ valant de 15 à 20, on peut signer avec quatre triplets GQ2 produits en parallèle ; avec $(k-1).m$ valant 60 ou plus, on peut signer avec un seul triplet GQ2. Par exemple, avec $k = 9$ et $m = 8$, un seul triplet GQ2 suffit ; chaque défi

comporte huit octets et les nombres de base sont 2, 3, 5, 7, 11, 13, 17 et 19.

L'opération de signature est une séquence de trois actes : un acte d'engagement, un acte de défi et un acte de réponse. Chaque acte produit un ou plusieurs triplets GQ2 comprenant chacun : un engagement R ($\neq 0$), un défi d composé de m défis élémentaires notés par d_1, d_2, ... d_m et une réponse D ($\neq 0$).

Le signataire dispose d'une fonction de hachage, du paramètre k et de la clé privée GQ2, c'est-à-dire, de la factorisation du module n selon l'une des trois représentations évoquées ci-dessus. **Au sein du signataire, on peut isoler un témoin qui exécute les actes d'engagement et de réponse**, de manière à isoler les fonctions et les paramètres les plus sensibles du démonstrateur. Pour calculer engagements et réponses, le témoin dispose du paramètre k et de la clé privée GQ2, c'est-à-dire, de la factorisation du module n selon l'une des trois représentations évoquées ci-dessus. Le témoin ainsi isolé est semblable au témoin défini au sein du démonstrateur. Il peut correspondre à une réalisation particulière, par exemple, • une carte à puce reliée à un PC formant ensemble le signataire, ou encore, • des programmes particulièrement protégés au sein d'un PC, ou encore, • des programmes particulièrement protégés au sein d'une carte à puce.

1) L'acte d'engagement comprend les opérations suivantes.

Lorsque le témoin dispose des m valeurs privées de Q_1 à Q_m et du module n, il tire au hasard et en privé un ou plusieurs aléas r ($0 < r < n$) ; puis, par k élévations successives au carré (mod n), il transforme chaque aléa r en un engagement R.

$$R \equiv r^v \pmod{n}$$

Lorsque le témoin dispose des f facteurs premiers de p_1 à p_f et des mf composantes privées $Q_{i,j}$, il tire au hasard et en privé une ou plusieurs collections de f aléas : chaque collection comporte un aléa r_i par facteur premier p_i ($0 < r_i < p_i$) ; puis, par k élévations successives au carré (mod p_i),

il transforme chaque aléa r_i en une composante d'engagement R_i.

$$R_i \equiv r_i^v \pmod{p_i}$$

Pour chaque collection de f composantes d'engagement, le témoin établit un engagement selon la technique des restes chinois. Il y a autant d'engagements que de collections d'aléas.

$$R = \text{Restes Chinois}(R_1, R_2, \ldots R_f)$$

2) L'acte de défi consiste à hacher tous les engagements R et le message à signer M pour obtenir un code de hachage à partir duquel le signataire forme un ou plusieurs défis comprenant chacun m défis élémentaires ; chaque défi élémentaire prend une valeur de 0 à $v/2-1$; par exemple, avec $k = 9$ et $m = 8$, chaque défi comporte huit octets. Il y a autant de défis que d'engagements.

$$d = d_1\ d_2 \ldots\ d_m, \text{ extraits du résultat Hash}(M, R)$$

3) L'acte de réponse comporte les opérations suivantes.

Lorsque la témoin dispose des m valeurs privées de Q_1 à Q_m et du module n, il calcule une ou plusieurs réponses D en utilisant chaque aléa r de l'acte d'engagement et les valeurs privées selon les défis élémentaires.

$$X \equiv Q_1^{d_1}.Q_2^{d_2}...Q_m^{d_m} \pmod{n}$$

$$D \equiv r.X \pmod{n}$$

Lorsque le témoin dispose des f facteurs premiers de p_1 à p_f et des $m.f$ composantes privées $Q_{i,j}$, il calcule une ou plusieurs collections de f composantes de réponse en utilisant chaque collection d'aléas de l'acte d'engagement : chaque collection de composantes de réponse comporte une composante par facteur premier.

$$X_i \equiv Q_{1,i}^{d_1}.Q_{2,i}^{d_2}...Q_{m,i}^{d_m} \pmod{p_i}$$

$$D_i \equiv r_i.X_i \pmod{p_i}$$

Pour chaque collection de composantes de réponse, le témoin établit une réponse selon la technique des restes chinois. Il y a autant de réponses que de défis.

$$D = \text{Restes Chinois}(D_1, D_2, \ldots D_f)$$

Le signataire signe le message M en lui adjoignant un appendice de signature comprenant :

- ou bien, chaque triplet GQ2, c'est-à-dire, chaque engagement R, chaque défi d et chaque réponse D,
- ou bien, chaque engagement R et chaque réponse D correspondante,
- ou bien, chaque défi d et chaque réponse D correspondante.

Le déroulement de l'opération de vérification dépend du contenu de l'appendice de signature. On distingue les trois cas.

Au cas où l'appendice comprend un ou plusieurs triplets, l'opération de contrôle comporte deux processus indépendants dont la chronologie est indifférente. Le contrôleur accepte le message signé si et seulement si les deux conditions suivantes sont remplies.

D'une part, chaque triplet doit être cohérent (une relation appropriée du type suivant doit être vérifiée) et recevable (la comparaison doit se faire sur une valeur non nulle).

$$R.\prod_{i=1}^{m} G_i^{d_i} \equiv D^{2^k} \pmod{n} \quad \text{ou bien} \quad R \equiv D^{2^k}.\prod_{i=1}^{m} G_i^{d_i} \pmod{n}$$

Par exemple, on transforme la réponse D par une séquence d'opérations élémentaires : k carrés (mod n) séparés par k–1 multiplications ou divisions (mod n) par des nombres de base. Pour la i ième multiplication ou division, qui s'effectue entre le i ième carré et le i+1 ième carré, le i ième bit du défi élémentaire d_1 indique s'il faut utiliser g_1, le i ième bit du défi élémentaire d_2 indique s'il faut utiliser g_2, ... jusqu'au i ième bit du défi élémentaire d_m qui indique s'il faut utiliser g_m. On doit ainsi retrouver chaque engagement R présent dans l'appendice de signature.

D'autre part, le ou les triplets doivent être liés au message M. En hachant tous les engagements R et le message M, on obtient un code de hachage à partir duquel on doit retrouver chaque défi d.

$d = d_1\ d_2 \ldots d_m$, identiques à ceux extraits du résultat Hash(M, R)

Au cas où l'appendice ne comprend pas de défi, l'opération de contrôle commence par la reconstitution de un ou plusieurs défis d' en hachant tous les engagements R et le message M.

$d' = d'_1\ d'_2 \ldots d'_m$, extraits du résultat Hash(M, R)

Ensuite, le contrôleur accepte le message signé si et seulement si chaque triplet est cohérent (une relation appropriée du type suivant est vérifiée) et recevable (la comparaison se fait sur une valeur non nulle).

$$R.\prod_{i=1}^{m} G_i^{d'_i} \equiv D^{2^k} \pmod{n} \quad \text{ou bien} \quad R \equiv D^{2^k}.\prod_{i=1}^{m} G_i^{d'_i} \pmod{n}$$

Au cas où l'appendice ne comprend pas d'engagement, l'opération de contrôle commence par la reconstitution de un ou plusieurs engagements R' selon une des deux formules suivantes, celle qui est appropriée. Aucun engagement rétabli ne doit être nul.

$$R' \equiv D^{2^k} / \prod_{i=1}^{m} G_i^{d_i} \pmod{n} \quad \text{ou bien} \quad R' \equiv D^{2^k}.\prod_{i=1}^{m} G_i^{d_i} \pmod{n}$$

Ensuite, le contrôleur doit hacher tous les engagements R' et le message M de façon à reconstituer chaque défis d.

$d = d_1\ d_2 \ldots d_m$, identiques à ceux extraits du résultat Hash(M, R')

Le contrôleur accepte le message signé si et seulement si chaque défi reconstitué est identique au défi correspondant figurant en appendice.

Dans la présente demande, on a montré qu'il existait des couples de valeurs privée Q et publique G permettant de mettre en œuvre le procédé, le système et le dispositif selon l'invention destiné à prouver l'authenticité d'une entité et/ou l'intégrité et/ou l'authenticité d'un message.

Dans la demande pendante déposée le même jour que la présente demande

par France Télécom, TDF et la Société Math RiZK et ayant pour inventeurs Louis Guillou et Jean-Jacques Quisquater, on a décrit un procédé pour produire des jeux de clés GQ2, à savoir, des modules n et des couples de valeurs publique G et privée Q dans le cas où l'exposant v est égal à 2^k. Elle est incorporée ici par référence.

Cette description détaillée de l'invention dans le cas où $v = 2^k$ est susceptible d'être généralisée à d'autres valeurs de v. C'est d'ailleurs ce qui a été exposé, en contrepoint aux revendications, dans les premières pages de la description concernant le cas où v est différent de 2^k. Pour autant que cela soit nécessaire, notamment pour des raisons ressortant des règles d'écriture d'une demande de brevet, et qu'il faille également dans cette partie de la description expliciter l'invention dans le cas où v est différent de 2^k, les premières pages de la description seront également supposées avoir été insérées à la suite de ce paragraphe.

Revendications

1. Procédé destiné à prouver à une entité contrôleur,

- l'authenticité d'une entité et/ou
- l'intégrité d'un message **M** associé à cette entité,

au moyen de tout ou partie des paramètres suivants ou dérivés de ceux-ci:

- **m** couples de valeurs privées $Q_1, Q_2, \ldots Q_m$ et publiques $G_1, G_2, \ldots G_m$ (**m** étant supérieur ou égal à 1),
- un module public **n** constitué par le produit de **f** facteurs premiers $p_1, p_2, \ldots p_f$ (**f** étant supérieur ou égal à 2),
- un exposant public **v** ;

ledit module, ledit exposant et lesdites valeurs étant liés par des relations du type :

$$G_i \cdot Q_i^v \equiv 1 \ . \bmod n \text{ ou } G_i \equiv Q_i^v \bmod n \ ;$$

ledit procédé met en œuvre selon les étapes suivantes une entité appelée témoin disposant des **f** facteurs premiers p_i et/ou des paramètres des restes chinois des facteurs premiers et/ou du module public **n** et/ou des **m** valeurs privées Q_i et/ou des **f.m** composantes $Q_{i,j}$ ($Q_{i,j} \equiv Q_i \bmod p_j$) des valeurs privées Q_i et de l'exposant public **v** ;

- le témoin calcule des engagements **R** dans l'anneau des entiers modulo **n** ; chaque engagement étant calculé en effectuant des opérations du type

$$R_i \equiv r_i^v \bmod p_i$$

où r_i est un aléa associé au nombre premier p_i tel que $0 < r_i < p_i$, chaque r_i appartenant à une collection d'aléas $\{r_1 , r_2 , \ldots r_f\}$, puis en appliquant la méthode des restes chinois,

- le témoin reçoit un ou plusieurs défis **d** ; chaque défi **d** comportant **m** entiers d_i ci-après appelés défis élémentaires ; le témoin calcule à partir de chaque défi **d** une réponse **D** en effectuant des opérations du type :

$$D_i \equiv r_i \cdot Q_{i,1}^{\,d1} \cdot Q_{i,2}^{\,d2} \cdot \ldots Q_{i,m}^{\,dm} \bmod p_i$$

puis en appliquant la méthode des restes chinois ;

ledit procédé étant tel qu'il y a autant de réponses **D** que de défis **d** que d'engagements **R**, chaque groupe de nombres **R, d, D** constituant un triplet noté **{R, d, D}**.

2. Procédé selon la revendication 1 destiné à prouver l'authenticité d'une entité appelée démonstrateur à une entité appelée contrôleur, ladite entité démonstrateur comprenant le témoin ;

lesdites entités démonstrateur et contrôleur exécutant les étapes suivantes :

- **étape 1 : acte d'engagement R**

- à chaque appel, le témoin calcule chaque engagement **R** en appliquant le processus spécifié selon la revendication 1,

- le démonstrateur transmet au contrôleur tout ou partie de chaque engagement **R**,

- **étape 2 : acte de défi d**

- le contrôleur, après avoir reçu tout ou partie de chaque engagement **R**, produit des défis **d** en nombre égal au nombre d'engagements **R** et transmet les défis **d** au démonstrateur,

- **étape 3 : acte de réponse D**

- le témoin calcule des réponses **D** à partir des défis **d** en appliquant le processus spécifié selon la revendication 1,

- **étape 4 : acte de contrôle**

- le démonstrateur transmet chaque réponse **D** au contrôleur,

cas où le démonstrateur a transmis une partie de chaque engagement R

dans le cas où le démonstrateur a transmis une partie de chaque engagement **R**, le contrôleur, disposant des **m** valeurs publiques $G_1, G_2, \ldots G_m$, calcule à partir de chaque défi **d** et de chaque réponse **D** un engagement reconstruit **R'** satisfaisant à une relation du type :

$$R' \equiv G_1^{\,d1} \cdot G_2^{\,d2} \cdot \ldots G_m^{\,dm} \cdot D^v \bmod n$$

ou à une relation du type,

$$R' \equiv D^v / G_1^{d1} . G_2^{d2} . \ldots G_m^{dm} . \mathbf{mod\ n} ,$$

le contrôleur vérifie que chaque engagement reconstruit **R'** reproduit tout ou partie de chaque engagement **R** qui lui a été transmis,

cas où le démonstrateur a transmis l'intégralité de chaque engagement R

dans le cas où le démonstrateur a transmis l'intégralité de chaque engagement **R**, le contrôleur, disposant des **m** valeurs publiques $G_1, G_2, \ldots G_m$, vérifie que chaque engagement **R** satisfait à une relation du type :

$$R \equiv G_1^{d1} . G_2^{d2} . \ldots G_m^{dm} . D^v \mathbf{\ mod\ n}$$

ou à une relation du type,

$$R \equiv D^v / G_1^{d1} . G_2^{d2} . \ldots G_m^{dm} . \mathbf{mod\ n} .$$

3. Procédé selon la revendication 1 destiné à prouver à une entité appelée contrôleur l'intégrité d'un message **M** associé à une entité appelée démonstrateur, ladite entité démonstrateur comprenant le témoin ;

lesdites entités démonstrateur et contrôleur exécutant les étapes suivantes :

• **étape 1 : acte d'engagement R**

- à chaque appel, le témoin calcule chaque engagement **R** en appliquant le processus spécifié selon la revendication 1,

• **étape 2 : acte de défi d**

- le démonstrateur applique une fonction de hachage **h** ayant comme arguments le message **M** et tout ou partie de chaque engagement **R** pour calculer au moins un jeton **T**,

- le démonstrateur transmet le jeton **T** au contrôleur,

- le contrôleur, après avoir reçu un jeton **T**, produit des défis **d** en nombre égal au nombre d'engagements **R** et transmet les défis **d** au démonstrateur,

• **étape 3 : acte de réponse D**

- le témoin calcule des réponses **D** à partir des défis **d** en appliquant le processus spécifié selon la revendication 1,

• **étape 4 : acte de contrôle**

- le démonstrateur transmet chaque réponse **D** au contrôleur,
- le contrôleur, disposant des m valeurs publiques $G_1, G_2, \ldots G_m$, calcule à partir de chaque défi **d** et de chaque réponse **D** un engagement reconstruit **R'** satisfaisant à une relation du type :

$$R' \equiv G_1^{d1} . G_2^{d2} . \ldots G_m^{dm} . D^v \bmod n$$

ou à une relation du type :

$$R' \equiv D^v / G_1^{d1} . G_2^{d2} . \ldots G_m^{dm} . \bmod n$$

- puis le contrôleur applique la fonction de hachage **h** ayant comme arguments le message **M** et tout ou partie de chaque engagement reconstruit **R'** pour reconstruire le jeton **T'**,
- puis le contrôleur vérifie que le jeton **T'** est identique au jeton **T** transmis.

4. Procédé selon la revendication 1 destiné à produire la signature numérique d'un message **M** par une entité appelée entité signataire, ladite entité signataire comprenant le témoin ;

ladite entité signataire exécute une opération de signature en vue d'obtenir un message signé comprenant :

- le message **M**,
- les défis **d** et/ou les engagements **R**,
- les réponses **D** ;

ladite entité signataire exécute l'opération de signature en mettant en oeuvre les étapes suivantes :

• **étape 1 : acte d'engagement R**

- à chaque appel, le témoin calcule chaque engagement **R** en appliquant le processus spécifié selon la revendication 1,

• **étape 2 : acte de défi d**

- le signataire applique une fonction de hachage **h** ayant comme arguments le message **M** et chaque engagement **R** pour obtenir un train binaire,
- le signataire extrait de ce train binaire des défis **d** en nombre égal au

nombre d'engagements **R**,

• étape 3 : acte de réponse D

- le témoin calcule des réponses **D** à partir des défis **d** en appliquant le processus spécifié selon la revendication 1.

5. Procédé selon la revendication 4 destiné à prouver l'authenticité du message **M** en contrôlant, par une entité appelée contrôleur, le message signé;

ladite entité contrôleur disposant du message signé exécute une opération de contrôle en procédant comme suit :

• cas où le contrôleur dispose des engagements R, des défis d, des réponses D,

dans le cas où le contrôleur dispose des engagements **R**, des défis **d**, des réponses **D**,

•• le contrôleur vérifie que les engagements **R**, les défis **d** et les réponses **D** satisfont à des relations du type

$$R \equiv G_1^{d1} . G_2^{d2} . \ldots G_m^{dm} . D^v \bmod n$$

ou à des relations du type :

$$R \equiv D^v / G_1^{d1} . G_2^{d2} . \ldots G_m^{dm} . \bmod n$$

•• le contrôleur vérifie que le message **M**, les défis **d** et les engagements **R** satisfont à la fonction de hachage

$$d = h(M, R)$$

• cas où le contrôleur dispose des défis d et des réponses D

dans le cas où le contrôleur dispose des défis **d** et des réponses **D**,

•• le contrôleur reconstruit, à partir de chaque défi **d** et de chaque réponse **D**, des engagements **R'** satisfaisant à des relations du type :

$$R' \equiv G_1^{d1} . G_2^{d2} . \ldots G_m^{dm} . D^v \bmod n$$

ou à des relations du type :

$$R' \equiv D^v / G_1^{d1} . G_2^{d2} . \ldots G_m^{dm} . \bmod n$$

•• le contrôleur vérifie que le message **M** et les défis **d** satisfont à la

fonction de hachage

$$d = h(M, R')$$

• **cas où le contrôleur dispose des engagements R et des réponses D**

dans le cas où le contrôleur dispose des engagements **R** et des réponses **D**,

•• le contrôleur applique la fonction de hachage et reconstruit **d'**

$$d' = h(M, R)$$

•• le contrôleur vérifie que les engagements **R**, les défis **d'** et les réponses **D**, satisfont à des relations du type :

$$R \equiv G_1^{d'1} . G_2^{d'2} . \ldots G_m^{d'm} . D^v \bmod n$$

ou à des relations du type :

$$R \equiv D^v / G_1^{d'1} . G_2^{d'2} . \ldots G_m^{d'm} . \bmod n$$

6. Procédé selon l'une quelconque des revendications 1 à 5 tel que les composantes $Q_{i,1}$, $Q_{i,2}$, ... $Q_{i,f}$ des valeurs privées Q_i, sont des nombres tirés au hasard à raison d'une composante $Q_{i,j}$ ($Q_{i,j} \equiv Q_i \bmod p_j$) pour chacun desdits facteurs premiers p_j, lesdites valeurs privées Q_i pouvant être calculées à partir desdites composantes $Q_{i,1}$, $Q_{i,2}$ ... $Q_{i,f}$ par la méthode des restes chinois,

lesdites valeurs publiques G_i, étant calculées

• en effectuant des opérations du type

$$G_{i,j} \equiv Q_{i,j}^v \bmod p_j$$

• puis en appliquant la méthode des restes chinois pour établir G_i tel que

$$G_i . Q_i^v \equiv 1 . \bmod n \text{ ou } G_i \equiv Q_i^v \bmod n ;$$

7. Procédé selon la revendication 6 tel que l'exposant public de vérification **v** est un nombre premier,

8. Procédé selon l'une quelconque des revendications 1 à 5

ledit exposant **v** étant tel que

$$v = 2^k$$

où **k** est un paramètre de sécurité plus grand que 1 ;

ladite valeur publique G_i étant le carré g_i^2 d'un nombre de base g_i inférieur

aux **f** facteurs premiers $p_1, p_2, \ldots p_f$; le nombre de base g_i étant tel que :

les deux équations :

$$x^2 \equiv g_i \bmod n \qquad \text{et} \qquad x^2 \equiv -g_i \bmod n$$

n'ont pas de solution en x dans l'anneau des entiers modulo **n**

et tel que :

l'équation :

$$x^v \equiv g_i^2 \bmod n$$

a des solutions en x dans l'anneau des entiers modulo **n** .

9. Système destiné à prouver à un serveur contrôleur,

- l'authenticité d'une entité et/ou
- l'intégrité d'un message **M** associé à cette entité,

au moyen de tout ou partie des paramètres suivants ou dérivés de ceux-ci:

- **m** couples de valeurs privées $Q_1, Q_2, \ldots Q_m$ et publiques $G_1, G_2, \ldots G_m$ (**m** étant supérieur ou égal à 1),
- un module public **n** constitué par le produit de **f** facteurs premiers $p_1, p_2, \ldots p_f$ (**f** étant supérieur ou égal à 2),
- un exposant public **v** ;

ledit module, ledit exposant et lesdites valeurs étant liés par des relations du type :

$$G_i \cdot Q_i^v \equiv 1 \bmod n \text{ ou } G_i \equiv Q_i^v \bmod n \ ;$$

ledit système comprend un dispositif témoin, notamment contenu dans un objet nomade se présentant par exemple sous la forme d'une carte bancaire à microprocesseur,

le dispositif témoin comporte une zone mémoire contenant les **f** facteurs premiers p_i et/ou des paramètres des restes chinois des facteurs premiers et/ou du module public **n** et/ou des **m** valeurs privées Q_i et/ou des **f.m** composantes $Q_{i,j}$ ($Q_{i,j} \equiv Q_i \bmod p_j$) des valeurs privées Q_i et de l'exposant public **v** ;

le dispositif témoin comporte aussi :

- des moyens de production d'aléas, ci-après désignés les moyens de production d'aléas du dispositif témoin,

- des moyens de calcul, ci-après désignés les moyens de calcul des engagements **R** du dispositif témoin, pour calculer des engagements **R** dans l'anneau des entiers modulo **n** ; chaque engagement étant calculé en effectuant des opérations du type

$$R_i \equiv r_i^{v} \bmod p_i$$

où r_i est un aléa associé au nombre premier p_i tel que $0 < r_i < p_i$, chaque r_i appartenant à une collection d'aléas $\{r_1 , r_2 , \ldots r_f\}$ produits par les moyens de production d'aléas, puis en appliquant la méthode des restes chinois ;

le dispositif témoin comporte aussi :

- des moyens de réception, ci-après désignés les moyens de réception des défis **d** du dispositif témoin, pour recevoir un ou plusieurs défis **d** ; chaque défi **d** comportant **m** entiers d_i ci-après appelés défis élémentaires ;

- des moyens de calcul, ci-après désignés les moyens de calcul des réponses **D** du dispositif témoin, pour calculer à partir de chaque défi **d** une réponse **D** en effectuant des opérations du type :

$$D_i \equiv r_i \cdot Q_{i,1}^{\,d1} \cdot Q_{i,2}^{\,d2} \cdot \ldots Q_{i,m}^{\,dm} \bmod p_i$$

puis, en appliquant la méthode des restes chinois ;

- des moyens de transmission pour transmettre un ou plusieurs engagements **R** et une ou plusieurs réponses **D** ;

il y a autant de réponses **D** que de défis **d** que d'engagements **R**, chaque groupe de nombres **R, d, D** constituant un triplet noté **{R, d, D}.**

10. Système selon la revendication 9 destiné à prouver l'authenticité d'une entité appelée démonstrateur à une entité appelée contrôleur ;

ledit système étant tel qu'il comporte

- un dispositif démonstrateur associé à l'entité démonstrateur, ledit dispositif démonstrateur étant interconnecté au dispositif témoin par des moyens d'interconnexion et pouvant se présenter notamment sous la forme

de microcircuits logiques dans un objet nomade par exemple sous la forme d'un microprocesseur dans une carte bancaire à microprocesseur,

- un dispositif contrôleur associé à l'entité contrôleur ; ledit dispositif contrôleur se présentant notamment sous la forme d'un terminal ou d'un serveur distant ; ledit dispositif contrôleur comportant des moyens de connexion pour le connecter électriquement, électromagnétiquement, optiquement ou de manière acoustique, notamment via un réseau de communication informatique, au dispositif démonstrateur ;

ledit système permettant d'exécuter les étapes suivantes :

• **étape 1 : acte d'engagement R**

- à chaque appel, les moyens de calcul des engagements **R** du dispositif témoin calculent chaque engagement **R** en appliquant le processus spécifié selon la revendication 9,

- le dispositif témoin comporte des moyens de transmission, ci-après désignés les moyens de transmission du dispositif témoin, pour transmettre tout ou partie de chaque engagement **R** au dispositif démonstrateur, via les moyens d'interconnexion ;

- le dispositif démonstrateur comporte aussi des moyens de transmission, ci-après désigné les moyens de transmission du dispositif démonstrateur, pour transmettre tout ou partie de chaque engagement **R** au dispositif contrôleur, via les moyens de connexion ;

• **étape 2 : acte de défi d**

le dispositif contrôleur comporte des moyens de productions de défis pour produire, après avoir reçu tout ou partie de chaque engagement **R**, des défis **d** en nombre égal au nombre d'engagements **R**,

le dispositif contrôleur comporte aussi des moyens de transmission, ci-après désignés les moyens de transmission du contrôleur, pour transmettre les défis **d** au démonstrateur,

• **étape 3 : acte de réponse D**

les moyens de réception des défis **d** du dispositif témoin, reçoivent chaque défi **d** provenant du dispositif démonstrateur, via les moyens d'interconnexion,

les moyens de calcul des réponses **D** du dispositif témoin calculent les réponses **D** à partir des défis **d** en appliquant le processus spécifié selon la revendication 9,

• **étape 4 : acte de contrôle**

les moyens de transmission du démonstrateur transmettent chaque réponse **D** au contrôleur

le dispositif contrôleur comporte aussi

- des moyens de calcul, ci-après désignés les moyens de calcul du dispositif contrôleur,

- des moyens de comparaison, ci-après désignés les moyens de comparaison du dispositif contrôleur,

cas où le démonstrateur a transmis une partie de chaque engagement R

dans le cas où les moyens de transmission du démonstrateur ont transmis une partie de chaque engagement **R**, les moyens de calcul du dispositif contrôleur, disposant des **m** valeurs publiques $G_1, G_2, \ldots G_m$, calculent à partir de chaque défi **d** et de chaque réponse **D** un engagement reconstruit **R'** satisfaisant à une relation du type :

$$R' \equiv G_1^{d1} . G_2^{d2} . \ldots G_m^{dm} . D^v \bmod n$$

ou à une relation du type,

$$R' \equiv D^v / G_1^{d1} . G_2^{d2} . \ldots G_m^{dm} . \bmod n ,$$

les moyens de comparaison du dispositif contrôleur comparent chaque engagement reconstruit **R'** à tout ou partie de chaque engagement **R** reçus,

cas où le démonstrateur a transmis l'intégralité de chaque engagement R

dans le cas où les moyens de transmission du démonstrateur ont transmis l'intégralité de chaque engagement **R**, les moyens de calcul et les moyens

de comparaison du dispositif contrôleur, disposant des **m** valeurs publiques $G_1, G_2, \ldots G_m$, vérifient que chaque engagement **R** satisfait à une relation du type :

$$R \equiv G_1^{d1} . G_2^{d2} . \ldots G_m^{dm} . D^v \bmod n$$

ou à une relation du type,

$$R \equiv D^v / G_1^{d1} . G_2^{d2} . \ldots G_m^{dm} . \bmod n .$$

11. Système selon la revendication 9 destiné à prouver à une entité appelée contrôleur l'intégrité d'un message **M** associé à une entité appelée démonstrateur,

ledit système étant tel qu'il comporte

- un dispositif démonstrateur associé à l'entité démonstrateur, ledit dispositif démonstrateur étant interconnecté au dispositif témoin par des moyens d'interconnexion et pouvant se présenter notamment sous la forme de microcircuits logiques dans un objet nomade par exemple sous la forme d'un microprocesseur dans une carte bancaire à microprocesseur,

- un dispositif contrôleur associé à l'entité contrôleur ; ledit dispositif contrôleur se présentant notamment sous la forme d'un terminal ou d'un serveur distant ; ledit dispositif contrôleur comportant des moyens de connexion pour le connecter électriquement, électromagnétiquement, optiquement ou de manière acoustique, notamment via un réseau de communication informatique, au dispositif démonstrateur ;

ledit système permettant d'exécuter les étapes suivantes :

• **étape 1 : acte d'engagement R**

- à chaque appel, les moyens de calcul des engagements **R** du dispositif témoin calculent chaque engagement **R** en appliquant le processus spécifié selon la revendication 9,

- le dispositif témoin comporte des moyens de transmission, ci-après désignés les moyens de transmission du dispositif témoin, pour transmettre tout ou partie de chaque engagement **R** au dispositif démonstrateur, via les

moyens d'interconnexion ;

• **étape 2 : acte de défi d**

le dispositif démonstrateur comporte des moyens de calcul, ci-après désignés les moyens de calcul du dispositif démonstrateur, appliquant fonction de hachage **h** ayant comme arguments le message **M** et tout ou partie de chaque engagement **R** pour calculer au moins un jeton **T**,

le dispositif démonstrateur comporte aussi des moyens de transmission, ci-après désignés les moyens de transmission du démonstrateur, pour transmettre chaque jeton **T** , via les moyens de connexion, au dispositif au contrôleur,

le dispositif contrôleur comporte aussi des moyens de productions de défis pour produire, après avoir reçu le jeton **T**, les défis **d** en nombre égal au nombre d'engagements **R** ,

le dispositif contrôleur comporte aussi des moyens de transmission, ci-après désignés les moyens de transmission du dispositif contrôleur, pour transmettre les défis **d** au démonstrateur,

• **étape 3 : acte de réponse D**

les moyens de réception des défis **d** du dispositif témoin, reçoivent chaque défi **d** provenant du dispositif démonstrateur, via les moyens d'interconnexion,

les moyens de calcul des réponses **D** du dispositif témoin calculent les réponses **D** à partir des défis **d** en appliquant le processus spécifié selon la revendication 9,

• **étape 4 : acte de contrôle**

les moyens de transmission du démonstrateur transmettent chaque réponse **D** au contrôleur,

le dispositif contrôleur comporte aussi des moyens de calcul, ci-après désignés les moyens de calcul du dispositif contrôleur, disposant des **m** valeurs publiques G_1, G_2, ... G_m, pour d'une part, calculer à partir de

chaque défi **d** et de chaque réponse **D** un engagement reconstruit **R'** satisfaisant à une relation du type :

$$R' \equiv G_1^{d1} . G_2^{d2} . \ldots G_m^{dm} . D^v \bmod n$$

ou à une relation du type :

$$R' \equiv D^v / G_1^{d1} . G_2^{d2} . \ldots G_m^{dm} . \bmod n$$

puis d'autre part, calculer en appliquant la fonction de hachage **h** ayant comme arguments le message **M** et tout ou partie de chaque engagement reconstruit **R'**, un jeton **T'**,

le dispositif contrôleur comporte aussi des moyens de comparaison, ci-après désignés les moyens de comparaison du dispositif contrôleur, pour comparer le jeton **T'** au jeton **T** reçu.

12. Système selon la revendication 9 destiné à produire la signature numérique d'un message **M**, ci après désigné le message signé, par une entité appelée entité signataire,

le message signé comprenant :

- le message **M**,
- les défis **d** et/ou les engagements **R**,
- les réponses **D** ;

ledit système étant tel qu'il comporte un dispositif signataire associé à l'entité signataire, ledit dispositif signataire étant interconnecté au dispositif témoin par des moyens d'interconnexion et pouvant se présenter notamment sous la forme de microcircuits logiques dans un objet nomade par exemple sous la forme d'un microprocesseur dans une carte bancaire à microprocesseur,

ledit système permettant d'exécuter les étapes suivantes :

- **étape 1 : acte d'engagement R**

à chaque appel, les moyens de calcul des engagements **R** du dispositif témoin calculent chaque engagement **R** en appliquant le processus spécifié selon la revendication 9,

le dispositif témoin comporte des moyens de transmission, ci-après désignés les moyens de transmission du dispositif témoin, pour transmettre tout ou partie de chaque engagement **R** au dispositif signataire, via les moyens d'interconnexion;

• **étape 2 : acte de défi d**

le dispositif signataire comporte des moyens de calcul, ci-après désignés les moyens de calcul du dispositif signataire, appliquant une fonction d hachage **h** ayant comme arguments le message **M** et chaque engagement **R** pour calculer un train binaire et extraire de ce train binaire des défis **d** en nombre égal au nombre d'engagements **R,**

• **étape 3 : acte de réponse D**

les moyens de réception des défis **d** , reçoivent chaque défi **d** provenant du dispositif signataire, via les moyens d'interconnexion,

les moyens de calcul des réponses **D** du dispositif témoin calculent les réponses **D** à partir des défis **d** en appliquant le processus spécifié selon la revendication 9,

le dispositif témoin comporte des moyens de transmission, ci-après désignés les moyens de transmission du dispositif témoin, pour transmettre les réponses **D** au dispositif signataire, via les moyens d'interconnexion.

13. Système selon la revendication 11 destiné à prouver l'authenticité du message **M** en contrôlant, par une entité appelée contrôleur, le message signé;

ledit système étant tel qu'il comporte un dispositif contrôleur associé à l'entité contrôleur ; ledit dispositif contrôleur se présentant notamment sous la forme d'un terminal ou d'un serveur distant ; ledit dispositif contrôleur comportant des moyens de connexion pour le connecter électriquement, électromagnétiquement, optiquement ou de manière acoustique, notamment via un réseau de communication informatique, au dispositif démonstrateur ;

ledit dispositif signataire associé à l'entité signataire comporte des moyens

de transmission, ci-après désignés les moyens de transmission du dispositif signataire, pour transmettre au dispositif contrôleur, le message signé, via les moyens de connexion, de telle sorte que le dispositif contrôleur dispose d'un message signé comprenant:

- le message **M**,
- les défis **d** et/ou les engagements **R**,
- les réponse **D**

le dispositif contrôleur comporte :

- des moyens de calcul, ci-après désignés les moyens de calcul du dispositif contrôleur,
- des moyens de comparaison, ci-après désignés les moyens de comparaison du dispositif contrôleur,

• cas où le contrôleur dispose des engagements R, des défis d, des réponses D,

dans le cas où le dispositif contrôleur dispose des engagements **R,** des défis **d,** des réponses **D,**

• • les moyens de calcul et de comparaison du dispositif contrôleur vérifient que les engagements **R**, les défis **d** et les réponses **D** satisfont à des relations du type

$$\mathbf{R \equiv G_1^{\,d1} . G_2^{\,d2} . \ldots G_m^{\,dm} . D^v \bmod n}$$

ou à des relations du type :

$$\mathbf{R \equiv D^v / G_1^{\,d1} . G_2^{\,d2} . \ldots G_m^{\,dm} . \bmod n}$$

• • les moyens de calcul et de comparaison du dispositif contrôleur vérifient que le message **M**, les défis **d** et les engagements **R** satisfont à la fonction de hachage

$$\mathbf{d = h\,(M, R)}$$

• cas où le contrôleur dispose des défis d et des réponses D

dans le cas où le dispositif contrôleur dispose des défis **d** et des réponses **D,**

• • les moyens de calcul du dispositif contrôleur calculent, à partir de

chaque défi **d** et de chaque réponse **D**, des engagements **R'** satisfaisant à des relations du type :

$$R' \equiv G_1^{d1} . G_2^{d2} . \ldots G_m^{dm} . D^v \bmod n$$

ou à des relations du type :

$$R' \equiv D^v / G_1^{d1} . G_2^{d2} . \ldots G_m^{dm} . \bmod n$$

•• les moyens de calcul et de comparaison du dispositif contrôleur vérifie que le message **M** et les défis **d** satisfont à la fonction de hachage

$$d = h(M, R')$$

• cas où le contrôleur dispose des engagements R et des réponses D

dans le cas où le dispositif contrôleur dispose des engagements **R** et des réponses **D,**

•• les moyens de calcul du dispositif contrôleur appliquent la fonction de hachage et calculent **d'** tel que

$$d' = h(M, R)$$

•• les moyens de calcul et de comparaison du dispositif contrôleur vérifient que les engagements **R**, les défis **d'** et les réponses **D**, satisfont à des relations du type :

$$R \equiv G_1^{d'1} . G_2^{d'2} . \ldots G_m^{d'm} . D^v \bmod n$$

ou à des relations du type :

$$R \equiv D^v / G_1^{d'1} . G_2^{d'2} . \ldots G_m^{d'm} . \bmod n$$

14. Système selon l'une quelconque des revendications 9 à 13 tel que les composantes $Q_{i,1}$, $Q_{i,2}$, ... $Q_{i,f}$ des valeurs privées Q_i, sont des nombres tirés au hasard à raison d'une composante $Q_{i,j}$ ($Q_{i,j} \equiv Q_i \bmod p_j$) pour chacun desdits facteurs premiers p_j, lesdites valeurs privées Q_i pouvant être calculées à partir desdites composantes $Q_{i,1}$, $Q_{i,2}$ ... $Q_{i,f}$ par la méthode des restes chinois,

lesdites valeurs publiques G_i, étant calculées

• en effectuant des opérations du type

$$G_{i,j} \equiv Q_{i,j}^v \bmod p_j$$

• puis en appliquant la méthode des restes chinois pour établir G_i tel que

$$G_i \cdot Q_i^v \equiv 1 \cdot \mathbf{mod}\ n \text{ ou } G_i \equiv Q_i^{-v} \mathbf{mod}\ n ;$$

15. Système selon la revendication 14 tel que l'exposant public de vérification v est un nombre premier,

16. Système selon l'une quelconque des revendications 9 à 13

ledit exposant **v** étant tel que

$$v = 2^k$$

où **k** est un paramètre de sécurité plus grand que 1 ;

ladite valeur publique G_i étant le carré g_i^2 d'un nombre de base g_i inférieur aux **f** facteurs premiers $p_1, p_2, \ldots p_f$; le nombre de base g_i étant tel que :

les deux équations :

$$x^2 \equiv g_i \mathbf{mod}\ n \qquad \text{et} \qquad x^2 \equiv -g_i \mathbf{mod}\ n$$

n'ont pas de solution en x dans l'anneau des entiers modulo **n**

et tel que :

l'équation :

$$x^v \equiv g_i^2 \mathbf{mod}\ n$$

a des solutions en x dans l'anneau des entiers modulo **n** .

17. Dispositif terminal associé à une entité, se présentant notamment sous la forme d'un objet nomade par exemple sous la forme d'une carte bancaire à microprocesseur, destiné à prouver à dispositif contrôleur,

- l'authenticité d'une entité et/ou
- l'intégrité d'un message **M** associé à cette entité,

au moyen de tout ou partie des paramètres suivants ou dérivés de ceux-ci:

- **m** couples de valeurs privées $Q_1, Q_2, \ldots Q_m$ et publiques $G_1, G_2, \ldots G_m$ (**m** étant supérieur ou égal à 1),
- un module public **n** constitué par le produit de **f** facteurs premiers $p_1, p_2, \ldots p_f$ (**f** étant supérieur ou égal à 2),
- un exposant public **v** ;

ledit module, ledit exposant et lesdites valeurs étant liés par des relations du

type :

$$G_i \cdot Q_i^v \equiv 1 \cdot \mathbf{mod}\ n \text{ ou } G_i \equiv Q_i^v \mathbf{mod}\ n ;$$

ledit dispositif terminal comprend un dispositif témoin comportant une zone mémoire contenant les **f** facteurs premiers p_i et/ou des paramètres des restes chinois des facteurs premiers et/ou du module public **n** et/ou des **m** valeurs privées Q_i et/ou des **f.m** composantes $Q_{i,j}$ ($Q_{i,j} \equiv Q_i \mathbf{mod}\ p_j$) des valeurs privées Q_i et de l'exposant public **v** ;

le dispositif témoin comporte aussi :

- des moyens de production d'aléas, ci-après désignés les moyens de production d'aléas du dispositif témoin,

- des moyens de calcul, ci-après désignés les moyens de calcul des engagements **R** du dispositif témoin, pour calculer des engagements **R** dans l'anneau des entiers modulo **n** ; chaque engagement étant calculé en effectuant des opérations du type

$$R_i \equiv r_i^v \mathbf{mod}\ p_i$$

où r_i est un aléa associé au nombre premier p_i tel que $0 < r_i < p_i$, chaque r_i appartenant à une collection d'aléas $\{r_1 , r_2 , \ldots r_f\}$ produits par les moyens de production d'aléas, puis en appliquant la méthode des restes chinois ;

le dispositif témoin comporte aussi :

- des moyens de réception, ci-après désignés les moyens de réception des défis **d** du dispositif témoin, pour recevoir un ou plusieurs défis **d** ; chaque défi **d** comportant **m** entiers d_i ci-après appelés défis élémentaires ;

- des moyens de calcul, ci-après désignés les moyens de calcul des réponses **D** du dispositif témoin, pour calculer à partir de chaque défi **d** une réponse **D** en effectuant des opérations du type :

$$D_i \equiv r_i \cdot Q_{i,1}^{\ d1} \cdot Q_{i,2}^{\ d2} \cdot \ldots Q_{i,m}^{\ dm} \mathbf{mod}\ p_i$$

puis, en appliquant la méthode des restes chinois ;

- des moyens de transmission pour transmettre un ou plusieurs engagements **R** et une ou plusieurs réponses **D** ;

il y a autant de réponses **D** que de défis **d** que d'engagements **R**, chaque groupe de nombres **R, d, D** constituant un triplet noté **{R, d, D}.**

18. Dispositif terminal selon la revendication 17 destiné à prouver l'authenticité d'une entité appelée démonstrateur à une entité appelée contrôleur ;

ledit dispositif terminal étant tel qu'il comporte un dispositif démonstrateur associé à l'entité démonstrateur, ledit dispositif démonstrateur étant interconnecté au dispositif témoin par des moyens d'interconnexion et pouvant se présenter notamment sous la forme de microcircuits logiques dans un objet nomade par exemple sous la forme d'un microprocesseur dans une carte bancaire à microprocesseur,

ledit dispositif démonstrateur comportant des moyens de connexion pour le connecter électriquement, électromagnétiquement, optiquement ou de manière acoustique, notamment via un réseau de communication informatique, à un dispositif contrôleur associé à l'entité contrôleur ; ledit dispositif contrôleur se présentant notamment sous la forme d'un terminal ou d'un serveur distant ;

ledit dispositif terminal permettant d'exécuter les étapes suivantes :

- **étape 1 : acte d'engagement R**

- à chaque appel, les moyens de calcul des engagements **R** du dispositif témoin calculent chaque engagement **R** en appliquant le processus spécifié selon la revendication 17,

- le dispositif témoin comporte des moyens de transmission, ci-après désignés les moyens de transmission du dispositif témoin, pour transmettre tout ou partie de chaque engagement **R** au dispositif démonstrateur, via les moyens d'interconnexion ;

le dispositif démonstrateur comporte aussi des moyens de transmission, ci-après désignés les moyens de transmission du démonstrateur, pour transmettre tout ou partie de chaque engagement **R** au dispositif contrôleur,

via les moyens de connexion,

• **étape 2 et 3 : acte de défi d, acte de réponse D**

les moyens de réception des défis **d** du dispositif témoin, reçoivent chaque défi **d** provenant du dispositif contrôleur via les moyens de connexion entre le dispositif contrôleur et le dispositif démonstrateur et via les moyens d'interconnexion entre le dispositif démonstrateur et le dispositif témoin,

les moyens de calcul des réponses **D** du dispositif témoin calculent les réponses **D** à partir des défis **d** en appliquant le processus spécifié selon la revendication 17,

• **étape 4 : acte de contrôle**

les moyens de transmission du démonstrateur transmettent chaque réponse **D** au dispositif contrôleur qui procède au contrôle.

19. Dispositif terminal selon la revendication 17 destiné à prouver à une entité appelée contrôleur l'intégrité d'un message **M** associé à une entité appelée démonstrateur,

ledit dispositif terminal étant tel qu'il comporte un dispositif démonstrateur associé à l'entité démonstrateur, ledit dispositif démonstrateur étant interconnecté au dispositif témoin par des moyens d'interconnexion et pouvant se présenter notamment sous la forme de microcircuits logiques dans un objet nomade par exemple sous la forme d'un microprocesseur dans une carte bancaire à microprocesseur,

ledit dispositif démonstrateur comportant des moyens de connexion pour le connecter électriquement, électromagnétiquement, optiquement ou de manière acoustique, notamment via un réseau de communication informatique, à un dispositif contrôleur associé à l'entité contrôleur ; ledit dispositif contrôleur se présentant notamment sous la forme d'un terminal ou d'un serveur distant ;

ledit dispositif terminal permettant d'exécuter les étapes suivantes :

• **étape 1 : acte d'engagement R**

- à chaque appel, les moyens de calcul des engagements **R** du dispositif témoin calculent chaque engagement **R** en appliquant le processus spécifié selon la revendication 17,

- le dispositif témoin comporte des moyens de transmission, ci-après désignés les moyens de transmission du dispositif témoin, pour transmettre tout ou partie de chaque engagement **R** au dispositif démonstrateur, via les moyens d'interconnexion ;

• **étape 2 et 3 : acte de défi d, acte de réponse**

le dispositif démonstrateur comporte des moyens de calcul, ci-après désignés les moyens de calcul du dispositif démonstrateur, appliquant fonction de hachage **h** ayant comme arguments le message **M** et tout ou partie de chaque engagement **R** pour calculer au moins un jeton **T**,

le dispositif démonstrateur comporte aussi des moyens de transmission, ci-après désignés les moyens de transmission du démonstrateur, pour transmettre chaque jeton **T** , via les moyens de connexion, au dispositif au contrôleur,

les moyens de réception des défis **d** du dispositif témoin, reçoivent chaque défi **d** provenant du dispositif démonstrateur, via les moyens d'interconnexion,

les moyens de calcul des réponses **D** du dispositif témoin calculent les réponses **D** à partir des défis **d** en appliquant le processus spécifié selon la revendication 17,

• **étape 4 : acte de contrôle**

les moyens de transmission du démonstrateur transmettent chaque réponse **D** au dispositif contrôleur qui procède au contrôle.

20. Dispositif terminal selon la revendication 17 destiné à produire la signature numérique d'un message **M**, ci après désigné le message signé, par une entité appelée entité signataire,

le message signé comprenant :

- le message **M**,
- les défis **d** et/ou les engagements **R**,
- les réponses **D** ;

ledit dispositif terminal étant tel qu'il comporte un dispositif signataire associé à l'entité signataire, ledit dispositif signataire étant interconnecté au dispositif témoin par des moyens d'interconnexion et pouvant se présenter notamment sous la forme de microcircuits logiques dans un objet nomade par exemple sous la forme d'un microprocesseur dans une carte bancaire à microprocesseur,

ledit dispositif signataire comportant des moyens de connexion pour le connecter électriquement, électromagnétiquement, optiquement ou de manière acoustique, notamment via un réseau de communication informatique, à un dispositif contrôleur associé à l'entité contrôleur ; ledit dispositif contrôleur se présentant notamment sous la forme d'un terminal ou d'un serveur distant ;

ledit dispositif terminal permettant d'exécuter les étapes suivantes :

- **étape 1 : acte d'engagement R**

à chaque appel, les moyens de calcul des engagements **R** du dispositif témoin calculent chaque engagement **R** en appliquant le processus spécifié selon la revendication 17,

le dispositif témoin comporte des moyens de transmission, ci-après désignés les moyens de transmission du dispositif témoin, pour transmettre tout ou partie de chaque engagement **R** au dispositif signataire, via les moyens d'interconnexion;

- **étape 2 : acte de défi d**

le dispositif signataire comporte des moyens de calcul, ci-après désignés les moyens de calcul du dispositif signataire, appliquant une fonction d hachage **h** ayant comme arguments le message **M** et chaque engagement **R** pour calculer un train binaire et extraire de ce train binaire des défis **d** en

nombre égal au nombre d'engagements **R**,

• **étape 3 : acte de réponse D**

les moyens de réception des défis **d** reçoivent les défis **d** provenant du dispositif signataire, via les moyens d'interconnexion,

les moyens de calcul des réponses **D** du dispositif témoin calculent les réponses **D** à partir des défis **d** en appliquant le processus spécifié selon la revendication 9,

le dispositif témoin comporte des moyens de transmission, ci-après désignés les moyens de transmission du dispositif témoin, pour transmettre les réponses **D** au dispositif signataire, via les moyens d'interconnexion.

21. Dispositif contrôleur, se présentant notamment sous la forme d'un terminal ou d'un serveur distant, associé à une entité contrôleur, destiné à prouver à un serveur contrôleur,

- l'authenticité d'une entité et/ou
- l'intégrité d'un message **M** associé à cette entité,

au moyen de tout ou partie des paramètres suivants ou dérivés de ceux-ci:

- **m** couples de valeurs privées $Q_1, Q_2, \ldots Q_m$ et publiques $G_1, G_2, \ldots G_m$ (**m** étant supérieur ou égal à 1),
- un module public **n** constitué par le produit de **f** facteurs premiers $p_1, p_2, \ldots p_f$ (**f** étant supérieur ou égal à 2),
- un exposant public **v** ;

ledit module, ledit exposant et lesdites valeurs étant liés par des relations du type :

$$G_i \cdot Q_i^v \equiv 1 \ . \bmod n \text{ ou } G_i \equiv Q_i^{-v} \bmod n \ ;$$

où Q_i désigne une valeur privée, inconnue du dispositif contrôleur, associée à la valeur publique G_i .

22. Dispositif contrôleur selon la revendication 22 destiné à prouver l'authenticité d'une entité appelée démonstrateur à une entité appelée contrôleur ;

ledit dispositif contrôleur comportant des moyens de connexion pour le connecter électriquement, électromagnétiquement, optiquement ou de manière acoustique, notamment via un réseau de communication informatique, à un dispositif démonstrateur associé à l'entité démonstrateur;

ledit dispositif contrôleur permettant d'exécuter les étapes suivantes :

• **étape 1 et 2 : acte d'engagement R, acte de défi**

ledit dispositif contrôleur comporte aussi des moyens de réception de tout ou partie des engagements **R** provenant du dispositif démonstrateur, via les moyens de connexion,

le dispositif contrôleur comporte des moyens de productions de défis pour produire, après avoir reçu tout ou partie de chaque engagement **R**, des défis **d** en nombre égal au nombre d'engagements **R**, chaque défi **d** comportant **m** entiers $\mathbf{d}_i$, ci-après appelés défis élémentaires

le dispositif contrôleur comporte aussi des moyens de transmission, ci-après désignés les moyens de transmission du dispositif contrôleur, pour transmettre les défis **d** au démonstrateur, via les moyens de connexion,

• **étapes 3 et 4 : acte de réponse, acte de contrôle**

le dispositif contrôleur comporte aussi

- des moyens de réception des réponses **D** provenant du dispositif démonstrateur, via les moyens de connexion,

- des moyens de calcul, ci-après désignés les moyens de calcul du dispositif contrôleur,

- des moyens de comparaison, ci-après désignés les moyens de comparaison du dispositif contrôleur,

cas où le démonstrateur a transmis une partie de chaque engagement R

dans le cas où les moyens de réception du dispositif contrôleur ont reçus une partie de chaque engagement **R**, les moyens de calcul du dispositif contrôleur, disposant des **m** valeurs publiques $\mathbf{G}_1$, $\mathbf{G}_2$, ... $\mathbf{G}_m$, calculent à partir de chaque défi **d** et de chaque réponse **D** un engagement reconstruit

R' satisfaisant à une relation du type :

$$R' \equiv G_1^{d1} . G_2^{d2} . \ldots G_m^{dm} . D^v \bmod n$$

ou à une relation du type,

$$R' \equiv D^v / G_1^{d1} . G_2^{d2} . \ldots G_m^{dm} . \bmod n ,$$

les moyens de comparaison du dispositif contrôleur comparent chaque engagement reconstruit **R'** à tout ou partie de chaque engagement **R** reçus,

cas où le démonstrateur a transmis l'intégralité de chaque engagement R

dans le cas où les moyens de réception du dispositif contrôleur ont reçus l'intégralité de chaque engagement **R**, les moyens de calcul et les moyens de comparaison du dispositif contrôleur, disposant des **m** valeurs publiques $G_1, G_2, \ldots G_m$, vérifient que chaque engagement **R** satisfait à une relation du type :

$$R \equiv G_1^{d1} . G_2^{d2} . \ldots G_m^{dm} . D^v \bmod n$$

ou à une relation du type,

$$R \equiv D^v / G_1^{d1} . G_2^{d2} . \ldots G_m^{dm} . \bmod n .$$

23. Dispositif contrôleur selon la revendication 22 destiné à prouver l'intégrité d'un message **M** associé à une entité appelée démonstrateur,

ledit dispositif contrôleur comportant des moyens de connexion pour le connecter électriquement, électromagnétiquement, optiquement ou de manière acoustique, notamment via un réseau de communication informatique, à un dispositif démonstrateur associé à l'entité démonstrateur;

ledit dispositif contrôleur permettant d'exécuter les étapes suivantes :

- **étapes 1 et 2 : acte d'engagement R, acte de défi**

ledit dispositif contrôleur comporte aussi des moyens de réception de jetons **T** provenant du démonstrateur, via les moyens de connexion,

le dispositif contrôleur comporte aussi des moyens de productions de défis pour produire, après avoir reçu le jeton **T**, des défis **d** en nombre égal au nombre d'engagements **R** , chaque défi **d** comportant **m** entiers, ci-après

appelés les défis élémentaires,

le dispositif contrôleur comporte aussi des moyens de transmission, ci-après désignés les moyens de transmission du dispositif contrôleur, pour transmettre les défis **d** au démonstrateur, via les moyens de connexion,

• **étapes 3 et 4 : acte de réponse D, acte de contrôle**

le dispositif contrôleur comporte aussi :

- des moyens de réception des réponses **D** provenant du dispositif démonstrateur, via les moyens de connexion,

le dispositif contrôleur comporte aussi

- des moyens de calcul, ci-après désignés les moyens de calcul du dispositif contrôleur, disposant des **m** valeurs publiques G_1, G_2, ... G_m, pour d'une part, calculer à partir de chaque défi **d** et de chaque réponse **D** un engagement reconstruit **R'** satisfaisant à une relation du type :

$$R' \equiv G_1^{d1} . G_2^{d2} . \ldots G_m^{dm} . D^v \bmod n$$

ou à une relation du type :

$$R' \equiv D^v / G_1^{d1} . G_2^{d2} . \ldots G_m^{dm} . \bmod n$$

puis d'autre part, calculer en appliquant la fonction de hachage **h** ayant comme arguments le message **M** et tout ou partie de chaque engagement reconstruit **R'**, un jeton **T'**,

le dispositif contrôleur comporte aussi des moyens de comparaison, ci-après désignés les moyens de comparaison du dispositif contrôleur, pour comparer le jeton **T'** au jeton **T** reçu.

24. Dispositif contrôleur selon la revendication 22 destiné à prouver l'authenticité du message **M** en contrôlant, par une entité appelée contrôleur, le message signé;

le message signé, émis par un dispositif signataire associé à une entité signataire disposant d'une fonction de hachage **h (M, R)** ; comprenant:

- le message **M**,
- les défis **d** et/ou les engagements **R**,

- les réponse **D** ;

ledit dispositif contrôleur comportant des moyens de connexion pour le connecter électriquement, électromagnétiquement, optiquement ou de manière acoustique, notamment via un réseau de communication informatique, à un dispositif signataire associé à l'entité signataire ;

ledit dispositif contrôleur ayant reçu le message signé du dispositif signataire, via les moyens de connexion,

le dispositif contrôleur comporte :

- des moyens de calcul, ci-après désignés les moyens de calcul du dispositif contrôleur,

- des moyens de comparaison, ci-après désignés les moyens de comparaison du dispositif contrôleur,

• cas où le contrôleur dispose des engagements R, des défis d, des réponses D,

dans le cas où le dispositif contrôleur dispose des engagements **R,** des défis **d,** des réponses **D,**

•• les moyens de calcul et de comparaison du dispositif contrôleur vérifient que les engagements **R**, les défis **d** et les réponses **D** satisfont à des relations du type

$$\mathbf{R \equiv G_1^{\,d1} . G_2^{\,d2} . \ldots G_m^{\,dm} . D^v \bmod n}$$

ou à des relations du type :

$$\mathbf{R \equiv D^v / G_1^{\,d1} . G_2^{\,d2} . \ldots G_m^{\,dm} . \bmod n}$$

•• les moyens de calcul et de comparaison du dispositif contrôleur vérifient que le message **M,** les défis **d** et les engagements **R** satisfont à la fonction de hachage

$$\mathbf{d = h\,(M, R)}$$

• cas où le contrôleur dispose des défis d et des réponses D

dans le cas où le dispositif contrôleur dispose des défis **d** et des réponses **D,**

•• les moyens de calcul du dispositif contrôleur calculent, à partir de

chaque défi **d** et de chaque réponse **D**, des engagements **R'** satisfaisant à des relations du type :

$$R' \equiv G_1^{d1} . G_2^{d2} . \ldots G_m^{dm} . D^v \bmod n$$

ou à des relations du type :

$$R' \equiv D^v / G_1^{d1} . G_2^{d2} . \ldots G_m^{dm} . \bmod n$$

•• les moyens de calcul et de comparaison du dispositif contrôleur vérifie que le message **M** et les défis **d** satisfont à la fonction de hachage

$$d = h(M, R')$$

• cas où le contrôleur dispose des engagements R et des réponses D

dans le cas où le dispositif contrôleur dispose des engagements **R** et des réponses **D,**

•• les moyens de calcul du dispositif contrôleur appliquent la fonction de hachage et calculent **d'** tel que

$$d' = h(M, R)$$

•• les moyens de calcul et de comparaison du dispositif contrôleur vérifient que les engagements **R**, les défis **d'** et les réponses **D**, satisfont à des relations du type :

$$R \equiv G_1^{d'1} . G_2^{d'2} . \ldots G_m^{d'm} . D^v \bmod n$$

ou à des relations du type :

$$R \equiv D^v / G_1^{d'1} . G_2^{d'2} . \ldots G_m^{d'm} . \bmod n$$

(12) DEMANDE INTERNATIONALE PUBLIÉE EN VERTU DU TRAITÉ DE COOPÉRATION EN MATIÈRE DE BREVETS (PCT)

(19) Organisation Mondiale de la Propriété Intellectuelle
Bureau international

(43) Date de la publication internationale
10 août 2000 (10.08.2000)

PCT

(10) Numéro de publication internationale
WO 00/046946 A3

(51) Classification internationale des brevets[7] : H04L 9/32

(21) Numéro de la demande internationale :
PCT/FR00/00188

(22) Date de dépôt international :
27 janvier 2000 (27.01.2000)

(25) Langue de dépôt : français

(26) Langue de publication : français

(30) Données relatives à la priorité :

99/01065	27 janvier 1999 (27.01.1999)	FR
99/03770	23 mars 1999 (23.03.1999)	FR
99/12465	1 octobre 1999 (01.10.1999)	FR
99/12467	1 octobre 1999 (01.10.1999)	FR
99/12468	1 octobre 1999 (01.10.1999)	FR

(71) Déposants *(pour tous les États désignés sauf US)* : **FRANCE TELECOM** [FR/FR]; 6, place d'Alleray, F-75015 Paris (FR). **TELEDIFFUSION DE FRANCE** [FR/FR]; 10, rue d'Oradour-sur-Glane, F-75732 Paris Cedex 15 (FR). **MATH RIZK** [BE/BE]; Verte Voie 20, B-1348 Louvain-la-Neuve (BE).

(72) Inventeurs; et

(75) Inventeurs/Déposants *(pour US seulement)* : **GUILLOU, Louis** [FR/FR]; 16, rue de l'Ise, F-35230 Bourgbarre (FR). **QUISQUATER, Jean-Jacques** [BE/BE]; 3, avenue des Canards, B-1640 Rhode Saint Genese (BE).

(74) Mandataire : **VIDON, Patrice**; Cabinet Patrice Vidon, Immeuble Germanium, 80, avenue des Buttes de Coësmes, F-35700 Rennes (FR).

(81) États désignés *(national)* : AE, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CR, CU, CZ, DE, DK, DM, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZW.

(84) États désignés *(régional)* : brevet ARIPO (GH, GM, KE, LS, MW, SD, SL, SZ, TZ, UG, ZW), brevet eurasien (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), brevet européen (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), brevet OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

Publiée :
— *avec rapport de recherche internationale*

(88) Date de publication du rapport de recherche internationale: 10 octobre 2002

En ce qui concerne les codes à deux lettres et autres abréviations, se référer aux "Notes explicatives relatives aux codes et abréviations" figurant au début de chaque numéro ordinaire de la Gazette du PCT.

(54) **Title:** METHOD, SYSTEM, DEVICE FOR PROVING THE AUTHENTICITY OF AN ENTITY AND/OR THE INTEGRITY AND/OR THE AUTHENTICITY OF A MESSAGE

(54) **Titre :** PROCEDE, SYSTEME, DISPOSITIF DESTINES A PROUVER L'AUTHENTICITE D'UNE ENTITE ET/OU L'INTEGRITE ET/OU L'AUTHENTICITE D'UN MESSAGE

(57) **Abstract:** The proof is provided by the following parameters: m pairs of private values Q_i and public values P_i, m>1; a public module n formed by the product of f first factors p_i, f>2; a public exponent v, bound by the relationship of the type: $G_i.Q_i^v \equiv$ mod n or $G_i \equiv Q_i^v$ mod n.

(57) **Abrégé :** La preuve est établie au moyen des paramètres suivants: m couples de valeurs privées Q_i et publiques P_i,>1 un module public n constitué par le produit de f facteurs premiers p_i, f>2, un exposant public v, liés par des relations du type: $G_i.Q_i^v \equiv 1$ mod n ou $G_i \equiv Q_i^v$ mod n.

WO 00/046946 A3